UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	6517P002
First Inventor	Luc Vantalon, et al.
Title	Methods And Apparatuses For Secondary Conditional Access Server
Express Mail Label No.	EV 409355695 US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

1. ☒ Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. ☐ Applicant claims small entity status. See 37 CFR 1.27.
3. ☒ Specification *[Total Pages 96]* *(preferred arrangement set forth below)*
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. ☒ Drawing(s) *(35 U.S.C. 113)* *[Total Sheets 19]*
5. Oath or Declaration (signed) *[Total Pages 3]*
   a. ☒ Newly executed (original or copy)
   b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 18 completed)*
      i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ Application Data Sheet. See 37 CFR 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ paper
   c. ☐ Statements verifying identity of above copies

17858 U.S. PTO 11/007116

9. ☒ Assignment Papers (cover sheet & document(s))
10. ☐ 37 C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment ☐ Application Amended to Reflect Claim of Priority
14. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☒ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. ☐ Other: _____

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____

Prior application Information: Examiner _____ *Group/Art Unit:* _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

☒ *Customer Number* 08791 *or* ☐ *Correspondence address below*

Name	Blakely, Sokoloff, Taylor & Zafman LLP				
Address	12400 Wilshire Boulevard, 7th Floor				
City	Los Angeles	*State*	California	*Zip Code*	90025
Country		*Telephone*	(408) 720-8300	*Fax*	(408) 720-8383

Name (Print/Type)	Lehua Wang	*Registration No. (Attorney/Agent)*	48,023
Signature		*Date*	12/7/04

Based on PTO/SB/05 (04-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 06/04/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

IPR2025-00305
ASUS EX1002 Page 1

FEE TRANSMITTAL for FY 2004

Effective 10/01/2004. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($) 4,154.00

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Luc Vantalon
Examiner Name	
Art Unit	
Attorney Docket No.	6517P002

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☐ Credit any overpayments

☒ Charge any additional fee(s) or underpayment of fees as required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	790	2001	395	Utility filing fee	790.00
1002	350	2002	175	Design filing fee	
1003	550	2003	275	Plant filing fee	
1004	790	2004	395	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 790.00

2. EXTRA CLAIM FEES

	Extra Claims		Fee from below		Fee Paid
Total Claims	146 - 20* =	126	x 18.00	=	$2,268.00
Independent Claims	15 - 3* =	12	x 88.00	=	$1,056.00
Multiple Dependent				=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	88	2201	44	Independent claims in excess of 3
1203	300	2203	150	Multiple Dependent claim, if not paid
1204	88	2204	44	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 3,324.00

***or number previously paid, if greater, For Reissues, see below*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	430	2252	215	Extension for reply within second month	
1253	980	2253	490	Extension for reply within third month	
1254	1,530	2254	765	Extension for reply within fourth month	
1255	2,080	2255	1,040	Extension for reply within fifth month	
1404	340	2401	170	Notice of Appeal	
1402	340	2402	170	Filing a brief in support of an appeal	
1403	300	2403	150	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,370	2453	685	Petition to revive - unintentional	
1501	1,370	2501	685	Utility issue fee (or reissue)	
1502	490	2502	245	Design issue fee	
1503	660	2503	330	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Prosessing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	40.00
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 40.00

SUBMITTED BY

Complete (if applicable)

Name *(Print/Type)*	Lehua Wang	*Registration No. (Attorney/Agent)*	48,023	*Telephone*	(408) 720-8300
Signature				*Date*	12/7/04

Based on PTO/SB/17 (10-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 02/10/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

NONPUBLICATION REQUEST UNDER 35 U.S.C. 122(b)(2)(B)(i)		
	First Named Inventor	Luc Vantalon
	Title	Methods And Apparatuses For Secondary Conditional Access Server
	Attorney Docket Number	6517P002

I hereby certify that the invention disclosed in the attached application **has not and will not be** the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.

I hereby request that the attached application not be published under 35 U.S.C. 122(b).

1-17-04
Date

Signature

(408) 720-8300
Telephone number

Lehua Wang, Reg. No. 48,023
Typed or printed name

This request must be signed in compliance with 37 CFR 1.33(b) and submitted with the application **upon filing**.

Applicant may rescind this nonpublication request at any time. If applicant rescinds a request that an application not be published under 35 U.S.C. 122(b), the application will be scheduled for publication at eighteen months from the earliest claimed filing date for which a benefit is claimed.

If applicant subsequently files an application directed to the invention disclosed in the attached application in another country, or under a multilateral international agreement, that requires publication of applications eighteen months after filing, the applicant **must** notify the United States Patent and Trademark Office of such filing within forty-five (45) days after the date of the filing of such foreign or international application. **Failure to do so will result in abandonment of this application (35 U.S.C. 112(b)(2)(B)(iii)).**

Based on PTO/SB/35 (08-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 08/11/2003.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	6517P002
First Inventor	Luc Vantalon, et al.
Title	Methods And Apparatuses For Secondary Conditional Access Server
Express Mail Label No.	EV 409355695 US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

1. ☒ Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. ☐ Applicant claims small entity status. See 37 CFR 1.27.
3. ☒ Specification *[Total Pages 96]* *(preferred arrangement set forth below)*
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. ☒ Drawing(s) *(35 U.S.C. 113)* *[Total Sheets 19]*
5. Oath or Declaration (signed) *[Total Pages 3]*
   a. ☒ Newly executed (original or copy)
   b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 18 completed)*
      i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ Application Data Sheet. See 37 CFR 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ paper
   c. ☐ Statements verifying identity of above copies
9. ☒ Assignment Papers (cover sheet & document(s))
10. ☐ 37 C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment ☐ Application Amended to Reflect Claim of Priority
14. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☒ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. ☐ Other: _____

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____

Prior application Information: Examiner _____ *Group/Art Unit:* _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

☒ *Customer Number* 08791 *or* ☐ *Correspondence address below*

Name	Blakely, Sokoloff, Taylor & Zafman LLP				
Address	12400 Wilshire Boulevard, 7th Floor				
City	Los Angeles	*State*	California	*Zip Code*	90025
Country		*Telephone*	(408) 720-8300	*Fax*	(408) 720-8383

Name (Print/Type)	Lehua Wang	*Registration No. (Attorney/Agent)*	48,023
Signature		*Date*	12/7/04

Based on PTO/SB/05 (04-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 06/04/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FEE TRANSMITTAL for FY 2004

Effective 10/01/2004. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($) 4,154.00

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Luc Vantalon
Examiner Name	
Art Unit	
Attorney Docket No.	6517P002

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☐ Credit any overpayments

☒ Charge any additional fee(s) or underpayment of fees as required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	790	2001	395	Utility filing fee	790.00
1002	350	2002	175	Design filing fee	
1003	550	2003	275	Plant filing fee	
1004	790	2004	395	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 790.00

2. EXTRA CLAIM FEES

	Extra Claims		Fee from below		Fee Paid
Total Claims 146	- 20* =	126	x 18.00	=	$2,268.00
Independent Claims 15	- 3* =	12	x 88.00	=	$1,056.00
Multiple Dependent				=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	88	2201	44	Independent claims in excess of 3
1203	300	2203	150	Multiple Dependent claim, if not paid
1204	88	2204	44	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 3,324.00

***or number previously paid, if greater, For Reissues, see below*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	430	2252	215	Extension for reply within second month	
1253	980	2253	490	Extension for reply within third month	
1254	1,530	2254	765	Extension for reply within fourth month	
1255	2,080	2255	1,040	Extension for reply within fifth month	
1404	340	2401	170	Notice of Appeal	
1402	340	2402	170	Filing a brief in support of an appeal	
1403	300	2403	150	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,370	2453	685	Petition to revive - unintentional	
1501	1,370	2501	685	Utility issue fee (or reissue)	
1502	490	2502	245	Design issue fee	
1503	660	2503	330	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Prosessing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	40.00
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify)

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 40.00

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Lehua Wang	Registration No. (Attorney/Agent)	48,023	Telephone	(408) 720-8300
Signature				Date	12/7/04

Based on PTO/SB/17 (10-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 02/10/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

NONPUBLICATION REQUEST UNDER 35 U.S.C. 122(b)(2)(B)(i)		
	First Named Inventor	Luc Vantalon
	Title	Methods And Apparatuses For Secondary Conditional Access Server
	Attorney Docket Number	6517P002

I hereby certify that the invention disclosed in the attached application **has not and will not be** the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.

I hereby request that the attached application not be published under 35 U.S.C. 122(b).

1-17-04
Date

Signature

(408) 720-8300
Telephone number

Lehua Wang, Reg. No. 48,023
Typed or printed name

This request must be signed in compliance with 37 CFR 1.33(b) and submitted with the application **upon filing**.

Applicant may rescind this nonpublication request at any time. If applicant rescinds a request that an application not be published under 35 U.S.C. 122(b), the application will be scheduled for publication at eighteen months from the earliest claimed filing date for which a benefit is claimed.

If applicant subsequently files an application directed to the invention disclosed in the attached application in another country, or under a multilateral international agreement, that requires publication of applications eighteen months after filing, the applicant **must** notify the United States Patent and Trademark Office of such filing within forty-five (45) days after the date of the filing of such foreign or international application. **Failure to do so will result in abandonment of this application (35 U.S.C. 112(b)(2)(B)(iii)).**

Based on PTO/SB/35 (08-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 08/11/2003.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	6517P002
First Inventor	Luc Vantalon, et al.
Title	Methods And Apparatuses For Secondary Conditional Access Server
Express Mail Label No.	EV 409355695 US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

1. ☒ Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. ☐ Applicant claims small entity status. See 37 CFR 1.27.
3. ☒ Specification *[Total Pages 96]* *(preferred arrangement set forth below)*
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. ☒ Drawing(s) *(35 U.S.C. 113)* *[Total Sheets 19]*
5. Oath or Declaration (signed) *[Total Pages 3]*
   a. ☒ Newly executed (original or copy)
   b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 18 completed)*
      i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ Application Data Sheet. See 37 CFR 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ paper
   c. ☐ Statements verifying identity of above copies
9. ☒ Assignment Papers (cover sheet & document(s))
10. ☐ 37 C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment ☐ Application Amended to Reflect Claim of Priority
14. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☒ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. ☐ Other: _____

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____

Prior application Information: Examiner _____ *Group/Art Unit:* _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

☒ *Customer Number* 08791 *or* ☐ *Correspondence address below*

Name	Blakely, Sokoloff, Taylor & Zafman LLP				
Address	12400 Wilshire Boulevard, 7th Floor				
City	Los Angeles	*State*	California	*Zip Code*	90025
Country		*Telephone*	(408) 720-8300	*Fax*	(408) 720-8383

Name (Print/Type)	Lehua Wang	*Registration No. (Attorney/Agent)*	48,023
Signature		*Date*	12/7/04

Based on PTO/SB/05 (04-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 06/04/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FEE TRANSMITTAL for FY 2004

Effective 10/01/2004. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($) 4,154.00

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Luc Vantalon
Examiner Name	
Art Unit	
Attorney Docket No.	6517P002

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☐ Credit any overpayments

☒ Charge any additional fee(s) or underpayment of fees as required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	790	2001	395	Utility filing fee	790.00
1002	350	2002	175	Design filing fee	
1003	550	2003	275	Plant filing fee	
1004	790	2004	395	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 790.00

2. EXTRA CLAIM FEES

	Extra Claims		Fee from below		Fee Paid
Total Claims	146 - 20* =	126	x 18.00	=	$2,268.00
Independent Claims	15 - 3* =	12	x 88.00	=	$1,056.00
Multiple Dependent				=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	88	2201	44	Independent claims in excess of 3
1203	300	2203	150	Multiple Dependent claim, if not paid
1204	88	2204	44	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 3,324.00

***or number previously paid, if greater, For Reissues, see below*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	430	2252	215	Extension for reply within second month	
1253	980	2253	490	Extension for reply within third month	
1254	1,530	2254	765	Extension for reply within fourth month	
1255	2,080	2255	1,040	Extension for reply within fifth month	
1404	340	2401	170	Notice of Appeal	
1402	340	2402	170	Filing a brief in support of an appeal	
1403	300	2403	150	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,370	2453	685	Petition to revive - unintentional	
1501	1,370	2501	685	Utility issue fee (or reissue)	
1502	490	2502	245	Design issue fee	
1503	660	2503	330	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Prosessing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	40.00
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 40.00

SUBMITTED BY

Complete (if applicable)

Name *(Print/Type)*	Lehua Wang	*Registration No. (Attorney/Agent)*	48,023	*Telephone*	(408) 720-8300
Signature				*Date*	12/7/04

Based on PTO/SB/17 (10-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 02/10/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

NONPUBLICATION REQUEST UNDER 35 U.S.C. 122(b)(2)(B)(i)		
	First Named Inventor	Luc Vantalon
	Title	Methods And Apparatuses For Secondary Conditional Access Server
	Attorney Docket Number	6517P002

I hereby certify that the invention disclosed in the attached application **has not and will not be** the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.

I hereby request that the attached application not be published under 35 U.S.C. 122(b).

1-17-04
Date

Signature

(408) 720-8300
Telephone number

Lehua Wang, Reg. No. 48,023
Typed or printed name

This request must be signed in compliance with 37 CFR 1.33(b) and submitted with the application **upon filing**.

Applicant may rescind this nonpublication request at any time. If applicant rescinds a request that an application not be published under 35 U.S.C. 122(b), the application will be scheduled for publication at eighteen months from the earliest claimed filing date for which a benefit is claimed.

If applicant subsequently files an application directed to the invention disclosed in the attached application in another country, or under a multilateral international agreement, that requires publication of applications eighteen months after filing, the applicant **must** notify the United States Patent and Trademark Office of such filing within forty-five (45) days after the date of the filing of such foreign or international application. **Failure to do so will result in abandonment of this application (35 U.S.C. 112(b)(2)(B)(iii)).**

Based on PTO/SB/35 (08-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 08/11/2003.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

06517.P002

UNITED STATES PATENT APPLICATION

FOR

METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

INVENTORS:

LUC VANTALON
PAOLO SICCARDO

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1026

(408) 720-8300

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EV 409355695 US

Date of Deposit: 12-7-04

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Joyce Klein
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

12-7-04
(Date signed)

METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

FIELD OF THE TECHNOLOGY

[0001] The invention relates to conditional access (CA) for systems such as a digital cable television system, a satellite television system, etc.

BACKGROUND

[0002] Conditional access (CA) is a technique for limiting the access of content (e.g., audiovisual works such as movies) to authorized users. For example, CA systems have been developed for cable TV and non-cable TV including digital television (DTV). In a CA system for digital television, the media content is scrambled (encrypted) using a standard algorithm before broadcasting. The key used for scrambling/descrambling the media content in a CA system is called a control word (CW). The control word is securely provided to the subscribers through entitlement control messages and entitlement management messages. A security device uses the control word to descramble (decrypt) the received media content.

[0003] Typically, the control word changes frequently (e.g., about every 0.1 second). To prevent unauthorized access, the control words are protected (scrambled/encrypted) using a service key (SK) when being broadcast. Only the security devices in possession of the service key can recover the control word for descrambling the media content protected by the CA system.

[0004] An entitlement control message (ECM) is typically used to broadcast the

control word in an encrypted form, which can be decrypted using the service key. The entitlement control message is checked against the access criteria in order to provide authorization. The control word is released if authorization is granted. Using the service key, the system can securely broadcast common information, such as the control word, to subscribers simultaneously without having to individually broadcast a message for each of the subscribers.

[0005] To individually manage each security device, each security device has a unique identity so that the CA system can broadcast a message specifically for one security device. An entitlement management message (EMM) typically contains the actual authorization data (e.g., entitlement) to authorize the security device for certain access criteria. Entitlement management messages are individually addressed to particular security devices. An entitlement management message may be only for one particular security device with a unique identity. The system broadcasts an entitlement management message for each of the entire population of the security devices to individually control the security devices. Typically, each security device has a unique, secrete user key (UK) so that an entitlement management message for one security device can only be decrypted using the unique user key of the security device.

[0006] Typically, the service key also changes periodically (e.g., once a month for subscription TV or once a movie for Pay-per-View). An entitlement management message can be used to send the service key to a particular security device for a subscriber. The CA system broadcasts an entitlement management message for each subscribing security device to deliver the service key. After the service key is

individually delivered to the subscribing security devices using the entitlement management messages, the CA system can broadcast the encrypted control words that can be decrypted using the service key.

[0007] Through the use of entitlement management messages and entitlement control messages, a CA system can offer capabilities such as pay-per-view (PPV), interactive features such as video-on-demand (VOD) and games, the ability to restrict access to certain material, and the ability to direct messages to specific receiving devices (e.g., set-top boxes with a smart card).

[0008] In digital television, the media content (e.g., video and audio signals) is converted into a digital form using the MPEG-2 format. The digital form of the media content of one program is multiplexed together with those of other programs for transmission so that multiple programs appear to be transmitted simultaneously. The CA system scrambles the digital form of programs and transmits the entitlement control messages and the entitlement management messages with the digital form of programs for broadcast either within the multiplex (e.g., Satellite) or through an out-of-band channel (e.g., Cable).

[0009] Typically, a set-top box (STB) at the receiving end descrambles the data stream and decodes the MPEG-2 data for viewing. A tuner portion of the STB receives the incoming signal, demodulates it and reconstitutes the transport stream, which contains many packets of information. The set-top box can de-multiplex the entitlement management messages and entitlement control messages and the media content. The data (e.g., service key and control word) contained in the entitlement management message and entitlement control message are used to descramble the

encrypted programming material. The set-top box then renders the MPEG-2 data for viewing.

[0010] A digital rights management (DRM) system manages rights digitally. Digital rights management uses encryption software to protect electronic information and prevent widespread distribution. In a typical digital rights management scheme, a DRM server software program wraps the digital content through encryption according to applicable policies. A DRM client software program unwraps the content and makes it accessible in accordance with its rights. The rights are typically distributed to clients separately from the wrapped electronic information. DRM clients may include desktop PCs, handhold devices, set-top boxes, mobile phones and other portable devices. In additional to encrypting/scrambling the digital content to limit the distribution, a digital rights management system may also provide the description, identification, trading, protection, monitoring and tracking of various forms of rights.

[0011] Content encryption is typically performed using symmetric key cryptography, while key encryption is typically using public/private key cryptography. In symmetric key cryptography, the same key is used to both encrypt and decrypt the content. In public/private key cryptography, different but related keys are used to encrypt and decrypt the content.

SUMMARY OF THE DESCRIPTION

[0012] Methods and apparatuses for bridging two security systems so that a primary security system can control premium content distribution to external devices secured by a secondary security system. Some embodiments of the present invention are summarized in this section.

[0013] In one embodiment of the present invention, the primary security system is a broadcast CA system, used to secure the distribution of premium content only to legitimate subscribers; and the secondary security system includes a digital rights management system used to secure the distribution of premium content only to the legitimate devices of the subscriber.

[0014] In one embodiment of the present invention, the primary security system is a broadcast CA system, used to secure the distribution of premium content only to legitimate local broadcasters; and the secondary security system includes another broadcast CA system, used to secure the re-distribution of premium content only to the legitimate local subscribers.

[0015] In one embodiment of the present invention, the primary security system is a digital rights management system, used to secure the distribution of premium content only to legitimate devices of the subscriber; and the secondary security system is another digital rights management system, used to secure the further distribution of premium content only to other devices of the subscribers not supporting the primary digital rights management system.

[0016] In at least some embodiments of the present invention, a primary CA

server provides entitlement data and/or decryption keys to multiple primary CA clients, along with some encrypted premium content. A secondary CA server acts as a legitimate primary CA client; the secondary CA server tries to recover the protected content and to provide with the protected content a new set of entitlement data and/or decryption keys consistent with the original entitlements to one or more secondary CA clients.

[0017] In one embodiment of the present invention, the secondary CA server may completely remove the primary security system encryption before processing it for distribution to the secondary CA clients; or may keep some or the totality of the primary security system encryption, still hand over it to the secondary CA client but add provision to the content so that it can be further authorized at playback time.

[0018] In one embodiment of the present invention, the primary CA server may enable the secondary CA server to first distribute protected but non-authorized content to secondary CA clients and then authorize it later.

[0019] In one aspect of the present invention, a method to control a presentation of content, includes: receiving a representation of content from a first CA server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access; and presenting the content, at a user's request, through a second CA server which is coupled to the first CA server. The presenting of the content is authorized through a client server relationship between the second and the first CA servers respectively. The second CA server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content. In one example, the content is presented by a

network client of the second CA server using the second set of cryptographic keys; and the first CA server provides the second CA server the first set of cryptographic keys for authorized use. In one example of an embodiment, the second CA server authorizes the network client to use the content through the digital rights management system in accordance with authorization to use received from the first CA server. In one example, the second CA server translates authorization to access the content from authorization received from the first CA server to authorization for the network client. In one example of an embodiment, the secondary CA server acts as a primary CA server to another CA server. In one example of an embodiment, the first CA server provides authorization to the second CA server according to an identity of the second CA server; the second CA server provides authorization to the client according to an identity of the client; and the first CA server is not aware of an identity of the client.

[0020] One aspect of the present invention includes a method for the secondary CA server to distribute protected but non-authorized content to secondary CA clients; and to enable the same clients to play back the content when later authorized by the primary CA server.

[0021] One aspect of the present invention includes a method for a secondary CA server to process entitlement management messages from a primary CA server and to transmit to secondary CA clients through a network connection access controlled data that is in an access controlled format and that is at least partially derived from the entitlement management messages. In one example of an embodiment, the secondary CA server has a user key representing a subscriber of

the primary security system; and processing the entitlement management messages includes: decrypting an entitlement management message to obtain a service key of the primary security system.

[0022] In one example of an embodiment, the method further includes: receiving, at the secondary CA server, an entitlement control message of the primary security system; and processing the entitlement control message to obtain a control word of the primary security system; where the access controlled data includes the control word. In one example, the access controlled data comprises a decrypted version of the entitlement control message.

[0023] In one example of an embodiment, the method further includes: receiving, at the secondary CA server, an entitlement control message of the primary security system; and processing the entitlement control message on the secondary CA server to generate a substitutive entitlement control message as a replacement of the entitlement control message; where the access controlled data includes the substitutive entitlement control message. In one example, the substitutive entitlement control message has a control word encrypted using a key of the secondary CA server. In one example, the substitutive entitlement control message is to be decrypted using a user key of the primary security system. In one example, the entitlement control message and the substitutive entitlement control message have a same control word. In another example, the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different. In one example, the access controlled data further includes the first and second control words.

[0024] In one example of an embodiment, the method further includes: receiving, at the secondary CA server, a first entitlement control message containing a first control word and content scrambled by the first control word; generating a second entitlement control message containing a second control word that is different from the first control word; and descrambling the content using the first control word and rescrambling the content by the second control word; where the access controlled data comprises the content rescrambled by the second control word and second entitlement control message. In one example, the method further includes: storing, at the secondary CA server, the content rescrambled by the second control word; and retrieving the content rescrambled by the second control word in response to a request from the secondary CA clients.

[0025] In another aspect of the present invention, a method to process media content provided by a primary security system, includes: receiving, at a secondary CA client from a secondary CA server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from entitlement management messages of the primary security system. In one example of an embodiment, the secondary CA client does not have a user key representing a subscriber of the primary security system. In one example of an embodiment, the access controlled format protects access to data using a digital rights management system.

[0026] In one example, the method further includes: automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data; descrambling and

recording the portion of the media content in response to a determination to descramble; and recording the portion of the media content without descrambling in response to a determination not to descramble.

[0027] In one example of an embodiment, the method further includes: sending, from the client of the secondary conditional server to the secondary CA server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form; where the access controlled data comprises the control word. In one example, the method further includes: descrambling media content using the control word; and storing the media content in a storage under protection of a secondary security system. In another example, the method further includes: descrambling media content using the control word; and rendering the media content for presentation. In one example, the entitlement control message is retrieved from a storage device; the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary CA client to the secondary conditional server and when the access controlled data is received at the secondary CA client. In one example, the access controlled data includes a decrypted version of the entitlement control message.

[0028] In one example of an embodiment, the access controlled data includes a result of descrambling media content scrambled by the primary security system.

[0029] In one example of an embodiment, the method further includes: receiving

a first entitlement control message for descrambling a portion of media content received from the primary security system; and sending the first entitlement control message from the secondary CA client to the secondary CA server through a network connection. The access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the second entitlement control message is stored with the portion of the media content. In one example, both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted for decryption using a key of the secondary CA server. In another example, the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further includes: descrambling the content using the first control word and rescrambling the content using the second control word.

[0030] The present invention includes methods and apparatuses which perform these methods, including data processing systems which perform these methods, and computer readable media which when executed on data processing systems cause the systems to perform these methods.

[0031] Other features of the present invention will be apparent from the accompanying drawings and from the detailed description which follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[0032] The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings in which like references indicate similar elements.

[0033] **Figure 1** shows a block diagram example of a data processing system which may be used with the present invention.

[0034] **Figures 2A** and **2B** shows a primary security system bridged to a secondary security system according to one embodiment of the present invention.

[0035] **Figure 3** illustrates a complex networked system with multiple primary security systems reaching multiple secondary security systems clients across a home network environment according to one embodiment of the present invention.

[0036] **Figure 4** illustrates a conditional access arrangement which may be used with the present invention.

[0037] **Figure 5** illustrates a system having a secondary CA server for providing control words to secondary CA clients according to one embodiment of the present invention.

[0038] **Figure 6** illustrates a system having a secondary CA server for providing media content to secondary CA clients according to one embodiment of the present invention.

[0039] **Figure 7** illustrates a system having a secondary CA server for decoding entitlement control messages for secondary CA clients according to one embodiment of the present invention.

[0040] **Figure 8** illustrates a system having a secondary CA server for providing substitutive entitlement control messages to secondary CA clients according to one embodiment of the present invention.

[0041] **Figure 9** illustrates a system having a secondary CA server for re-scrambling media content for secondary CA clients according to one embodiment of the present invention.

[0042] **Figure 10A** illustrates an authorization process for recorded media content according to one embodiment of the present invention.

[0043] **Figure 10B** illustrates a prior art scenario to access recorded content.

[0044] **Figure 10C** illustrates a scenario to access recorded content according to one embodiment of the present invention.

[0045] **Figure 11** illustrates a system in which a secondary CA server is configured to decode the control words for the captured media content retrieved from a storage device according to one embodiment of the present invention.

[0046] **Figure 12** illustrates a system in which a secondary CA server is configured to decode the control words for capturing media content into a storage device according to one embodiment of the present invention.

[0047] **Figure 13** illustrates a system in which a secondary CA server is configured to automatically decode the control words before capturing media content into a storage device, or after retrieving captured media content from the storage device, according to one embodiment of the present invention.

[0048] **Figure 14** illustrates a system in which a secondary CA server is configured to generate substitutive entitlement control messages and decode the

control words for the captured media content retrieved from a storage device according to one embodiment of the present invention.

[0049] **Figure 15** shows a method of using a secondary CA server according to one embodiment of the present invention.

[0050] **Figure 16** shows a detailed method of a secondary CA server according to one embodiment of the present invention.

EX1002 - Page 24
IPR2025-00305
ASUS EX1002 Page 24

DETAILED DESCRIPTION

[0051] The following description and drawings are illustrative of the invention and are not to be construed as limiting the invention. Numerous specific details are described to provide a thorough understanding of the present invention. However, in certain instances, well known or conventional details are not described in order to avoid obscuring the description of the present invention. References to one or an embodiment in the present disclosure are not necessarily references to the same embodiment; and, such references mean at least one.

[0052] **Figure 2A** shows a primary security system bridged to a secondary security system according to one embodiment of the present invention. In **Figure 2A**, the primary CA server (253) controls the access to the content in the primary security domain (251). The primary security domain (251) is typically a broadcast CA system. The primary CA server (253) transmits entitlement management messages and entitlement control messages so that only authorized clients, such as a subscriber's set top box (e.g., 257) can access (decrypt) the CA protected content.

[0053] In one embodiment of the present invention, a secondary CA server (255) bridges the primary security domain (251) and the secondary security domain (261). The secondary security domain typically includes a set of secondary CA clients (e.g., 271, 273, ..., 279). The bridge (259) typically passes CA protected content from the primary security domain (251) to the secondary security domain (261) so that the secondary CA clients (e.g., 271, 273, ..., 279) in the secondary security domain

under the control of the secondary CA server (255) in accordance with security messages provided by the primary security domain (251) to the secondary CA server (255). The secondary CA clients (e.g., 271, 273, ..., 279) rely on the secondary CA server (255) to obtain the content. The secondary CA server (255) is partially in the primary security domain (251), since the secondary CA server is capable of processing the control information for conditional access provided by the primary CA server (253). The secondary CA server (255) acts as a client of the primary security domain (251) and as a control information provider of the secondary security domain (261). According to the access terms and conditions given by the primary CA server (253), the secondary CA server (255) conditionally allows the secondary CA clients (e.g., 271, 273, ..., 279) to access the content.

[0054] For example, in **Figure 2A**, the bridge 259 may hand over the scrambled (encrypted) content to the secondary CA clients. To descramble (decrypt) the content, the secondary CA clients request information from the secondary CA server (255). For example, in one embodiment, the secondary CA server (255) provides control words for descrambling the content to the authorized secondary CA clients. The control words are provided under the protection of a DRM system in the secondary security domain (261). The secondary security domain can include another CA server (not shown). In **Figure 2A**, the bridge (259) may also be partially or completely combined within the secondary CA server (255) as a single physical component of a distributed system.

[0055] Note that in **Figure 2A**, a bridge and a further secondary CA server can be used to extend from the secondary domain (261) into another domain. For

example, the client (279) can be replaced with a bridge and a further secondary CA server in a way similar to the bridge (259) and secondary CA server (255) replacing a set top box. Such an approach can be used recursively to form a chain of security domains bridged through the use of a hierarchy of cascaded secondary CA servers.

[0056] In one embodiment of the present invention, the secondary security domain is for a localized network, such as a network within a home or hotel or other domain. Alternatively, the secondary security domain may include Internet.

[0057] **Figure 2B** illustrates a bridge (283) in relation with a secondary CA server (281). In **Figure 2B**, the secondary CA server processes security messages, such as CA messages from the primary security domain. In one embodiment of the present invention, the secondary CA server translates authorization from the primary security domain into authorization in the secondary security domain. The secondary CA server generates security message for the secondary security domain in accordance with authorization obtained from security messages in the primary security domain. Thus, entities not known in the primary security domain can be provisioned through the use of the secondary CA server, which has an identity known in the primary security domain and knows the entities in the secondary security domain. In one embodiment, the secondary CA server follows rules (e.g., CA messages) of the primary CA server to manage a secondary subscriber management system (SMS) that is different from the primary subscriber management system managed by the primary CA server. In one embodiment, the client identities and authentication methods used by the secondary CA server in the secondary subscriber management system are independent from those used by the

primary CA server in the primary subscriber management system. As a server in the secondary subscriber management system and a client in the primary subscriber management system, the secondary CA server bridges the two subscriber management systems. In one embodiment of the present invention, the CA servers support two different roots of trust for security. The secondary CA server and the primary CA server supports root of trust independent from each other. In one embodiment, the root of trust is used to authenticate clients; the client authentication in the secondary security domain is completely independent from the client authentication in the primary security domain; and the authorization to use in the secondary security domain is in accordance with the authorization to use conveyed in the primary security domain.

[0058] In **Figure 2B**, a number of components are illustrated for the bridge (283), such as a physical interface (285), a transcrambler (287) and another physical interface (289). For example, the physical interface (285) may be a tuner which converts the signals representing the CA protected content into a data format; the transcrambler (287) may convert the protected content from one protected (e.g., encrypted) format to another protected (e.g., encrypted) format; and the physical interface (289) may be a data network communication interface for transmitting the protected content to a client in the secondary security domain. The secondary CA server may receive information from the physical interface (285). The secondary CA server (281) may directly provide the content to the physical interface (289) in accordance with the authorization from the CA messages. The secondary CA server (281) may provide messages to control the operations of the transcrambler (287) and

physical interface (289) in accordance with the authorization derived from the CA messages. In general, a bridge may include more or less components than those illustrated in **Figure 2B**. For example, a bridge may have one or more of: as a tuner, a transcrambler, a transcoder, a physical interface, a network communication interface, a cable, a storage device, etc.

[0059] **Figure 3** illustrates a complex networked system with two primary security system sources (211 and 215) with their own primary CA servers (226 and 228), two secondary CA servers (227 and 225) and many secondary CA clients (207, 209, 217, 221, 231 and 233). In one embodiment of the present invention, a secondary CA server is used to provide services to a plurality of devices connected to a network (201), such as a local area network (LAN) or a wireless LAN. The network (201) may be partially a wired Ethernet in a home of a service subscriber with one or more wireless access points for mobile devices such as a personal data assistant (PDA), a palm computer, a notebook computer, or a cellular phone (e.g., connected to the network through a WiFi or Bluetooth connection). For example, in **Figure 3**, the PDA (243) connects to the access point (241) through the wireless connection (245) and further to other components through the network (201). The network may also be a network for an organization or a commercial establishment (e.g., a hotel or a motel chain), such as an intranet or a virtual private network.

[0060] In **Figure 3**, a cable TV secondary CA server (225) is used with the cable TV service. The cable primary CA server (228) couples with the cable headend (215) to provide the CA protected media content through the cable television transmission system to the cable TV bridges (e.g., 217 and 219) which may include

cable TV tuners. The cable TV bridges receive the data packages and de-multiplex the entitlement management messages and entitlement control messages and the scrambled media content. Under the control and with the help of the cable TV secondary CA server (225), the media content can be secured on a storage (e.g., 221, 223 or 235) for access by various devices which can play back the media content, such as the personal computer (233) the media player (231), or the PDA (243). The personal computer (233) typically displays the video content on the display device (239), such as a Cathode Ray Tube (CRT) monitor or a flat Liquid-Crystal Display (LCD) panel. The media player (231) typically presents the media content on a television set (237). A media player may also be integrated with a television set to form a network-ready digital television set.

[0061] In one embodiment, the cable TV secondary CA server provides services to descramble/decrypt the cable TV broadcast. The decrypted/descrambled information is protected in a digital rights management system so that the media content from the broadcast of the cable TV system can be used in an authorized way. When authorized, the content can be recorded and played back at any time on any device convenient to the user in accordance with the rights of the subscriber. For example, with a subscription to only one simultaneous use, a user may choose to use cable TV bridge (217) to receive the broadcast and view the program on the TV (247), or use cable TV bridge (219) to record the program on the storage (223) for playing back at a different time using the PDA (243), the personal computer (233) or the media player (231).

[0062] In **Figure 3**, a satellite TV secondary CA server (227) is used to provide

services to both the satellite TV bridge A (207) and the satellite TV bridge B (209). The satellite TV secondary CA server (227) may store the protected media content on its storage (229) or on other storage devices on the network, such as the storage (235) of the personal computer (233) or the storage (221). Typically, a satellite (211) broadcasts (213) the protected media content to a geographical area. Separate satellite dishes (e.g., 203 and 205) are used for different satellite bridges (e.g., 207 and 209) respectively.

[0063] Traditionally, to access two different channels simultaneously, two set-top boxes are used. Satellite set-top boxes are independent from each other. The satellite broadcasts to the two set-top boxes as if the set-top boxes were for two different subscribers. In one embodiment of the present invention, the satellite TV secondary CA server provides services to both the satellite TV bridges. The satellite TV secondary CA server (227), not the satellite TV bridges (207 and 209), has the data representing the subscriber. Thus, one subscriber needs only one unique identification for the operation of multiple tuners.

[0064] In one embodiment, different secondary CA servers are used to extend the services of different primary CA servers, since different primary CA systems typically use entirely different algorithms and protocols for the entitlement management messages and entitlement control messages. In one embodiment of the present invention, the different secondary CA servers are physically in one data processing device with different software and smart cards for the processing of the messages of different CA systems. Further, a secondary CA server may be integrated with a bridge, a storage device, a renderer (e.g., PDA 243, personal

computer 223, media player 231), or a combination of them. For example, the satellite TV secondary CA server may include a storage for recording media content, a bridge for interfacing with a satellite dish and a renderer for decoding the media content into standard video signals (for a television set and/or for a computer monitor).

[0065] Further details about various different arrangements of the components (e.g., secondary CA server, bridge, storage, renderer) and the operations of the components are provided below.

[0066] **Figure 4** illustrates a conditional access arrangement which may be used with the present invention. In one embodiment of the present invention, a secondary CA server contains a security device (307) which has a unique user key (331) to represent the subscriber. The user key (331) can be used to decrypt the entitlement management message (EMM) (301), which has the encrypted service key (311). In one embodiment of the present invention, the secondary CA server performs the EMM decryption (321) for secondary CA clients using the user key (331) to recover the service key (SK) (333). The entitlement control message (ECM) (303) contains the encrypted control word (313). In one embodiment of the present invention, the secondary CA server further performs the ECM decryption (323) using the service key (333) to recover the control word (CW) (335) for the secondary CA clients. The scrambled content (305) can be descrambled using the control word (335) to generate the content (337). In one embodiment, the secondary CA server provides the control word to an authorized secondary CA client to descramble the content (305). Alternatively, the secondary CA server may further include a descrambler

(325) to descramble the content for secondary CA clients.

[0067] The descrambler of a digital television system uses a standard algorithm (e.g., Common Scrambling for DVB, DES for Advanced Television Systems Committee (ATSC) standard (Conditional Access System for Terrestrial Broadcast)). The descrambler (325) can be conveniently located on any of the components (e.g., a bridge, a renderer or a storage).

[0068] In one embodiment of the present invention, a secondary CA server performs ECM decryption (323) and then generates a replacement entitlement control message. The replacement entitlement control is encrypted for decryption using a different service key, which is under the control of the secondary CA server, so that the secondary CA server does not need to maintain the service key (333) for recorded contents. The replacement entitlement control can be recorded with the scrambled content (305) protected by the DRM system for later use.

[0069] In one embodiment of the present invention, the control word is further changed for recording. After the descrambler (325) generates the clear content (337), the clear content is re-scrambled using a different control word for recording. For the recorded content, the CA protection may be translated so that the control word may change in-frequently (e.g., one control word for one entire movie).

[0070] Typically, a secondary CA server performs both EMM decryption (321) and ECM decryption (323) for all the secondary CA clients (e.g., a bridge, a renderer or a storage), since both the ECM and EMM are specific to a particular CA system.

[0071] In one embodiment of the present invention, the results of a secondary

CA server are protected using a DRM system; and the DRM system manages the rights according to the data in the EMM (and/or ECM).

[0072] Although **Figure 4** shows a particular encryption/decryption arrangement of a CA system, it is understood that different arrangements can also be used with the present invention. For example, in a CA system, the service key may be delivered physically instead of through broadcasting. In general, the entitlement management messages are broadcast to individual devices to individually authorize entitlement; and the entitlement control messages are typically broadcast to all devices to provide the common key for descrambling the broadcast stream. It is understood that a service key represents the entitlement recovered from the entitlement management message; and the control word represents the key recovered from the entitlement control message for descrambling the media content.

[0073] **Figure 5** illustrates a system having a secondary CA server for providing control words to secondary CA clients according to one embodiment of the present invention. In **Figure 5**, the secondary CA server (431) uses its user key (UK 433) to recover the control word from the encrypted entitlement management message (EMM 435) and entitlement control message (ECM 437) for the secondary CA clients over the network (439). The recovered control word (441) is protected using a DRM system; and only a secondary CA client with appropriate rights (443) can use the control word (445) to descramble the content (447) to obtain the clear content (449) that is not encrypted/scrambled.

[0074] The rights to the control word can be determined from the data in the EMM at the time of recording and/or at the time of playback. The control word can

also be provided to the secondary CA clients in real time as the broadcast is received for immediate viewing.

[0075] Since the control word is provided through the network (439) which may cause unpredictable network communication delay, arrangement is made to synchronize the control word with the decoding of the media content. In one embodiment, the secondary CA client synchronizes the control word obtained from the server with the stream of media content for descrambling operation. In one embodiment of the present invention, a secondary CA client for playing back the media content buffers a time period worth of content in a pipeline for playback in anticipation of unpredictable network delay in obtaining the control word, which changes frequently (e.g., every 0.1 second). When a control word is delay, the descrambled content in the pipeline decreases and the scrambled content in the pipeline increases; when the control word is received, the descrambling operation resumes to increase the descrambled content in the pipeline and decrease the scrambled content in the pipeline. Thus, the buffering allows the secondary CA client to maintain a constant rate of descrambled content for rendering in real time.

[0076] In one embodiment of the present invention, a secondary CA server further includes a descrambler so that the secondary CA clients do not need a descrambler.

[0077] In one embodiment of the present invention, the secondary CA server (431) uses both the data in the EMM received prior to the content reception and the data in the EMM received prior to the content consumption, if different, to determine the rights of the user for the service key. For example, in one embodiment

of the present invention, when the user is entitled to the content at the time of recording, the service key can be recovered for the data in the EMM at the time of recording. When the recorded content is retrieved from the storage for playback, the secondary CA server may further determine the rights according to the data in the EMM for the current time period. In one embodiment, for example, the user is entitled to view the recorded content only if the user is currently a valid subscriber of the service (e.g., subscribing for the viewing of recorded contents). Alternatively, the secondary CA server uses only the data in the EMM at the time of recording to determine the rights to the recorded contents.

[0078] In one embodiment of the present invention, a primary CA server provides entitlement only at playback time. For example, the system can allow the user to record programs that the user is not entitled to use at the time of recording. After the user obtains the required rights (e.g., through purchase for pay-per-view, or upgrading a subscription package), the user can then playback the recorded information at any convenient time.

[0079] Generally, different CA systems (e.g., primary or secondary CA servers) have entirely different implementations of EMM and ECM but similar or same descramblers for content protection (e.g., according to the ATSC Standard). In one embodiment of the present invention, a secondary CA server decodes both the EMM and ECM and other client components process the content in standard formats (e.g., using a standard descrambling algorithm).

[0080] **Figure 6** illustrates a system having a secondary CA server for providing media content to secondary CA clients according to one embodiment of the present

invention. In **Figure 6**, the secondary CA server (461) has a user key (463) to decrypt the encrypted entitlement management message (EMM 471) and the encrypted entitlement control message (ECM 473) and the scrambled content (475). The secondary CA server descrambles the content and provides the DRM protected content (467) through the network (465) so that only the secondary CA client with the appropriate rights (469) can use the content (477).

[0081] In one embodiment of the present invention, the secondary CA server (461) includes one or more bridges and a storage device. The content can be recorded and stored in the storage device for later viewing or provided for real time use. The secondary CA server may directly record the original CA protected content, or record the descrambled content (with encryption for DRM protection), or record the content with substitutive CA protection (e.g., with replacement entitlement control message, or rescrambling using a different control word). In one embodiment of the present invention, the DRM protected content (467) is provided to the secondary CA clients according to the rights determined from EMM (and/or ECM) messages (e.g., at the time of recording and/or the time of playback).

[0082] **Figure 7** illustrates a system having a secondary CA server for decoding entitlement control messages for secondary CA clients according to one embodiment of the present invention. In **Figure 7**, the secondary CA server (501) with the user key (503) decodes the entitlement management message (EMM 507) and the entitlement control message (ECM_a 509) to provide, over the network (505), the local entitlement control message (ECM_b 511), which is protected under a DRM system. The secondary CA client with the rights (513) to the local entitlement

control message (ECM_b 511) can use the control word (515) in ECM_b (511) to descramble the content (517). Typically, the secondary CA client sends the local entitlement control message (ECM_b 511) back at the playback time for the control word (515) and then generates the clear content (519) using the control word (515) received from the secondary CA server (501). In one embodiment, the clear content (519) is rescrambled using a different scheme before stored on a storage. Alternatively, the descrambled content (519) can be recorded and stored in a storage under the protection of a DRM system.

[0083] Alternatively, a storage records the scrambled content (517) with the DRM protected ECM_b (511) so that a device with rights (513) can retrieve the media content (517) and ECM_b (511) for viewing at a different time. The decoded entitlement control message ECM_b (511) may be used to replace the original encrypted entitlement control message ECM_a (509) to generate a stream for storage and access under the DRM system. Since the use of the decoded entitlement control message (ECM_b 511) does not require the service key of the primary security system, the management of the recorded content can be simplified.

[0084] In one embodiment of the present invention, a secondary CA server generates substitutive entitlement control messages which are encrypted for decryption by a different service key that is managed by the secondary CA server (e.g., generated and maintained by the CA server). Typically, the CA system of a primary security system changes the service key periodically (e.g., once a month). Entitlement control messages recorded from different time periods need different service keys for decryption. In one embodiment of the present invention, to simplify

the service key management for the recorded content, a secondary CA server re-encrypts the entitlement control message to generate a substitutive entitlement control message for recording. The secondary CA server can later decrypt the substitutive entitlement control message without using the original service key.

[0085] **Figure 8** illustrates a system having a secondary CA server for providing substitutive entitlement control messages to secondary CA clients according to one embodiment of the present invention. In **Figure 8**, the secondary CA server (531) receives the entitlement management message (EMM 541) and the entitlement control message (ECM_a 543) which is to be decrypted using a service key (SK_a) provided by the EMM (541). The secondary CA server (531) decrypts the EMM (541) using the user key (533) to obtain the service key (SK_a) and then further decrypts the ECM_a (543) using the service key (SK_a) and obtains the control word (CW). The secondary CA server manages a service key SK_b (535) and re-encrypts the control word to create a local entitlement control message (ECM_b 545), which can then be decrypted using the service key SK_b (535). The decryption of the local entitlement control message ECM_b (545) does not need the original service key (SK_a) sent in the EMM (541). The secondary CA server (531) provides the ECM_b (545) as a substitutive entitlement control message to a secondary CA client through the network (537). The original entitlement control message (ECM_a 543) is replaced with the substitutive entitlement control message (ECM_b 545) to record and store the scrambled content (547) on the storage (539). When the scrambled content is retrieved from the storage (539) for use in a renderer, the secondary CA server (531) can decode the ECM_b (545) using the service key (SK_b 535) to retrieve the control

word in the ECM_b (545). The secondary CA server can then provide the control word to a secondary CA client in a way illustrated in **Figure 5**. The secondary CA server (531) may further determine whether or not to release the control word based on the entitlement management message received at the time of decrypting the substitutive control message (ECM_b 545). In one embodiment, the information stored on the storage (539) is further protected under a DRM system.

[0086] In a typical conditional access of a primary security system (e.g., digital TV or satellite TV), the control word changes frequently (e.g., once every 0.1 second). To protect the recorded and stored content, which may be further protected under a DRM system, it may not be necessary to change the control word as frequently. For example, an entire recorded movie may be rescrambled using one control word. In one embodiment of the present invention, a secondary CA server is used to descramble and re-scramble the CA protected content for recording.

[0087] **Figure 9** illustrates a system having a secondary CA server for re-scrambling media content for secondary CA clients according to one embodiment of the present invention. In **Figure 9**, the secondary CA server (561) receives the broadcast, including the entitlement management message (EMM 571), the entitlement control message (ECM_a 573) and the scrambled content (575). The secondary CA server (561) uses the user key (563) to access the data in EMM (571) (e.g., recovering the service key), to access the data in ECM_a (573) (e.g., recovering the control word), and to descramble the content (575). The secondary CA server (561) then rescrambles the content (e.g., using a different control word) and provides the rescrambled content (569) with the new entitlement management message

IPR2025-00305
ASUS EX1002 Page 40

(ECM_b 567) to one or more secondary CA clients through the network (565). In one embodiment, the ECM_b (567) is protected under a DRM system so that only the secondary CA clients with appropriate rights (581) can challenge the secondary CA server by sending the ECM_b (567) at playback time and get in return the control word (CW_b 577) for descrambling the content (569) to recover the clear content (579). In one embodiment of the present invention, the ECM_b (567) is further encrypted for decryption with a substitutive service key in a way similar to that illustrated in **Figure 8**.

[0088] **Figure 10A** illustrates an authorization process for recorded media content according to one embodiment of the present invention. In **Figure 10A**, the primary CA system (e.g., a digital TV system, or a satellite TV system) first sends (731) an entitlement management message (EMM) requesting caching of a program. The user may not already subscribe to the program (e.g., a movie or a sport program). Thus, the device of the user may not be authorized to descramble the program. According to one embodiment of the present invention, the device of the user can record (743) the scrambled program after receiving the EMM that requests caching the program at a subscriber system. The primary CA system then starts (733) broadcasting the program. After a period of time based on the length of the program, the content providing system ends (735) broadcasting the program. During the period, the device of the user records (743) the scrambled program. Since the user is not a subscriber to the program, the device is not authorized to playback the scrambled content at the time of recording. After the recording, the user may be prompted for availability of the program. If the user requests (745) authorization

(which may be at any time) to use the recorded program, an authorization EMM (737) is generated. The authorization EMM may be generated locally at the device, in a way similar to impulse pay per view (IPPV), or generated after the user calls the operator to obtain the authorization, in a way similar to over the phone pay per view (OPPV), or generated after the device transmits the request to the CA system through a data connection, in a way similar to Video-on-Demand (VOD). Once the device obtains the authorization to playback the recorded program, the device can descramble the program for playback (747).

[0089] In one embodiment of the present invention, a secondary CA server is used to process and manage the EMM for secondary CA clients. The authorization for playback is requested and granted through the secondary CA server. In one embodiment, the primary CA server is aware of the secondary CA server as a subscriber. For example, the primary CA server is aware of the identity of the secondary CA server and provides authorization according to the subscription status of the secondary CA server. However, the primary CA server may not aware of the identities of the secondary CA clients. In one embodiment of the present invention, the secondary CA server translates the authorization obtained from the primary CA server into authorization for the clients of the secondary server in a way consistent with the policy of the primary CA server.

[0090] For example, the secondary CA server may not consume the content; and the secondary CA server may be used to authorize one of its clients to use the subscription and consume the content (e.g., playback the media content in real time or after the media content is recorded). Thus, the secondary CA server may

dynamically attach its subscriber identity to one of its clients so that the combined secondary CA server and the corresponding client, which is dynamically selected, can be viewed as a subscriber that is known to the primary CA server.

[0091] Further, the secondary CA server may translate access policies in other sophisticated ways. For example, the secondary CA server may determine the authorization of simultaneous access by multiple devices to the same or different media contents. For example, a subscriber may have a subscription to use two independent players to see different channels. Instead of providing the subscriber with two set top boxes with two different identities, the vendor can provide the subscriber with a secondary CA server, which has one identity and authorizes two players to play back the media content according to the authorization from the primary CA server based on the subscription.

[0092] **Figure 10B** illustrates a prior art scenario to access recorded content. In **Figure 10B**, a user device (755), such as a set top box, that has an identity recognized as a subscriber interacts with the primary CA server (753) directly in the authorization process. For example, after the primary CA server sends a request to cache a program to a recorder (751), which is typically a part of a set top box, CA protected media content (765) can be recorded in recorder (751). At the time of recording the user may not be entitled to view the media content. The CA protected media content can then be stored in the recorder (751) in a CA protected format. To use the media content (759), the user device needs authorization from the primary CA server. If the user device has not already obtained the authorization, the user device (755) requests (763) authorization to use in communication with the primary

CA server (753), which may then send an authorization message (761) to the user device. The request for authorization may be alternatively sent through a user phone call, or through a data link between the primary CA server (753) and the user device (755).

[0093] In **Figure 10C**, the identity of the client of primary CA server (753) is directly attached to the user device which may be authorized according to the identity to remove CA protection from the received media content and play back (consume) the media content.

[0094] **Figure 10C** illustrates a scenario to access recorded content according to one embodiment of the present invention. In **Figure 10C**, the authorization process is through the secondary CA server (772), which is a client of the primary CA server (773). The secondary CA server (772) has an identity recognized as a subscriber of the primary CA server (773). The secondary CA server (772) may forward, translate, and/or manage its authorization received from the primary CA server (773) into authorization for its clients, such as the media player (775). Thus, even though the media player (775) may not have an identity recognizable as a client of the primary CA server (773), through the secondary CA server (772) the media player (775) is effectively recognized as a legitimate subscriber. Thus, one embodiment of the present invention allows the dynamic integration of two devices (e.g., the secondary CA server and a media player) into one logical entity, which may provide the functionality of a traditional set top box.

[0095] Further, one embodiment of the present invention allows the separation of the identity of the client of primary CA server (753) in one device (e.g., a

secondary CA server) and a user device which may be authorized according to the identity to remove CA protection from the received media content and/or play back the media content. Such an arrangement allows enormous flexibility in a content delivery system according to one embodiment of the present invention. For example, the media player (775) may use a different content protection system, such as a DRM system; the primary CA server don't have to support all media players of its users/subscribers; and the secondary CA sever can be used to extend the service and functionality of the primary CA system. Further, for example, the user can copy the protected content and move it to other storage medium and still be able to watch the content through the control of the secondary CA server. For example, the protected content can be distributed on a local network (e.g., within a home, a hotel, a campus, a building, etc.) through various available communication tools, media and protocols while the rights to use the protected content can be managed though the control of the secondary CA server in accordance with the authorization the secondary CA server obtained from the primary CA server.

[0096] In one embodiment, the secondary CA server (772) provides the authorization to its clients in a way consistent with the authorization it obtained from the primary CA server (773). Thus, the secondary CA server (772) conveys legitimate rights to its clients in accordance with the authorization from the primary CA server (773) without providing illegitimate access.

[0097] For example, in **Figure 10C**, the primary CA server may request (777) the recorder (771) to cache a program. The recorder (771) then records the CA protected media content (785) for later retrieval. The recorder (771) can be a device

separated from the secondary CA server (772) and the media player (775), or a component integrated within the secondary CA server (772) or the media player (775). To play back the media content (779), the media player (775) requests (789) authorization to use from the secondary CA server (772), since the media player (775) is not a direct client of the primary CA server (773). If the secondary CA server (772) has not yet obtained the authorization, the secondary CA server (772) sends an authorization request (787) to the primary CA server (773), which can then provide an authorization message (781) to the secondary CA server (772) based on the identity of the secondary CA server (772) as a client of the primary CA server (773). The secondary CA server then sends an authorization message (783) to the media player (775) based on the identity of the media player (775) as a client of the secondary CA server (772), in accordance with the authorization message (781) received from the primary CA server (773).

[0098] In one embodiment of the present invention, a secondary CA server has data to represent a subscriber. The secondary CA server is used to processing the entitlement management message and/or the entitlement control message of the primary CA server. A bridge interfaces with the primary security system to reconstitute the data stream, including the entitlement management message, the entitlement control message and the scrambled content. A storage is used to store the content for playing back at a different time. A renderer is used to process the content for presentation. Since the content is typically control word scrambled/descrambled using a standard algorithm, a standard scrambler/descrambler can be continently located on the conditional access, the bridge, or the renderer, depending on the

network configuration and/or other considerations.

[0099] Although some of the figures (e.g., **Figures 11 – 14**) and descriptions show a secondary CA server, a bridge, a storage, a renderer separately, it is understood that a secondary CA server, a bridge, a storage, a renderer can be physically combined in various different ways. The communication between these components is not necessarily all through network connections. For example, a secondary CA server may be physically separate from a bridge and a renderer and communicating to the bridge and renderer through a network; and the bridge and the renderer may be physically separated from each other or combined in one device. Alternatively, the secondary CA server may be combined with a bridge, communicating with a renderer over a network, or be combined with a renderer, communicating with a bridge over a network. The storage may be connected through a network to a secondary CA server, a bridge and a renderer, which may be combined in various ways as illustrated above. Alternatively, the storage may be in at least one of the secondary CA server, the bridge and the renderer and connected to the rest of the components through a network. Further, a storage may partially in one component and partially in another. As illustrated in **Figure 3**, a networked system may have multiple bridges, multiple renderers and multiple storages. Typically, one secondary CA server is a client of one primary CA server. However, one secondary CA server may also be a client of multiple CA systems.

[00100] In one embodiment of the present invention, a secondary CA server is used on a network to provide services to secondary CA clients. For example, a secondary CA server may decode entitlement management messages to determine

rights for a DRM system, decode entitlement control messages to recover control words for secondary CA clients, generate substitutive entitlement control messages, descramble CA protected contents for secondary CA clients, rescramble CA protected contents for secondary CA clients, etc.

[00101] **Figure 11** illustrates a system in which a secondary CA server is configured to decode the control words for the captured media content retrieved from a storage device according to one embodiment of the present invention. In **Figure 11**, the bridge (603) interfaces with the primary security system to receive the broadcast feed (601), including the user key (UK) protected entitlement management message (EMM 615), the service key (SK) protected entitlement control message (ECM 613) and the control word (CW) scrambled content (611).

[00102] The bridge (603) may include one or more components, such as a tuner, a transcrambler, a transcoder, a physical interface, a network communication interface, a cable, a storage device, etc.

[00103] The bridge (603) sends the entitlement management message (627) to the secondary CA server (609), which has the user key (621) that represents the identity of the subscriber. The secondary CA server (609) determines the entitlement of the subscriber to the content from the entitlement management message (627). For example, the secondary CA server (609) uses the user key (621) to retrieve the service key from the entitlement management message (627). The storage (605) stores the content and the entitlement control message (617) under the protection of a DRM system.

[00104] Although **Figure 11** shows a link between the bridge (603) and the

storage (605), it is understood that the recording of the content is not necessary through a direct path from the bridge to the storage. For example, the content and the entitlement control message may be sent to the secondary CA server, which then records the content into the storage (605) in accordance to the data in EMM (627). The storage (605) can be physically integrated within the secondary CA server (609). Alternatively, or in addition, the bridge (603) may be physically integrated within the secondary CA server (609).

[00105] In one embodiment of the present invention, only the content that the subscriber is entitled to according to the EMM at the time of recording is recorded into the storage (605). For example, the storage (605) may be a separate network device or integrated within the bridge (603); and the secondary CA server (609) authorizes the bridge (603) to record the content in accordance with the entitlement of the EMM (627).

[00106] In one embodiment of the present invention, the bridge records the content on the storage. In one embodiment, the bridge records only the content that the subscriber is entitled to use at the time of recording. Based on the data in EMM (627), the secondary CA server determines whether or not the subscriber is entitled to use the scrambled content and sends a message to the bridge about the determination. The secondary CA server maintains data derived from the EMM (627), such as the service key, so that the recorded content can be later decrypted/descrambled after the recorded content is retrieved from the storage (605) for use.

[00107] Alternatively, the bridge may record the scrambled content and the

entitlement control message regardless the entitlement. The secondary CA server maintains data derived from the EMM (627), such as the service key, so that the recorded content can be later correlated with the corresponding data derived from the EMM (627) for decryption/descrambling operations.

[00108] After the renderer (607) retrieves the recorded content and the associated entitlement control message (617) from the storage (605), the renderer (605) sends the entitlement control message (625) to the secondary CA server (609) protected by the DRM system. The secondary CA server (609) decodes the entitlement control message (625) and releases the control word (619) only when the access criteria are satisfied. The released control word (619) is protected under a DRM system so that only the renderer (607) with the appropriate rights (623) can use the released control word (619) to descramble the content retrieved from the storage (605).

[00109] In one embodiment of the present invention, the released control word (619) is access controlled according to the entitlement management message received for the time period when the content is recorded and/or according to the entitlement management message received for the time period when the content is retrieved for use. For example, a movie may be played back at any time after being recording if the subscriber is entitled to view it at the time of recording. Alternatively, a recorded movie may be viewed only if the user is a current subscriber. Thus, even if the user is authorized to play the movie at the time of recording, the secondary CA server still needs to verify that the user is currently a subscriber at the time of playback according to the entitlement management message for the current time period. In one embodiment of the present invention, a movie can

be recorded even if the subscriber is not entitled to view it at the time of recording, since the entitlement may be obtained after the recording.

[00110] In one embodiment of the present invention, a CA system can send entitlement management messages for delayed authorization. For example, an entitlement management message may include a service key for the system to record the content without the authorization for playback. The secondary CA server (609) can manage the service key so that when the user is subsequently authorized to view the content, the CA system of the primary security system does not have to recall which service key was used for the recorded content. When the user obtains the authorization to view after the recording (e.g., through a pay-per-view scheme, or upgrading the subscription package), the secondary CA server (609) can decrypt the entitlement control message using the service key maintained by the secondary CA server.

[00111] In one embodiment of the present invention, the secondary CA server (609) communicates with the bridge (603) and the renderer (607) through a network connection. Alternatively, the secondary CA server (609) may communicate with either the bridge (603) or the renderer (607) through a network connection (e.g., when the secondary CA server is integrated with either the renderer or the bridge).

[00112] **Figure 12** illustrates a system in which a secondary CA server is configured to decode the control words for capturing media content into a storage device according to one embodiment of the present invention. In **Figure 12**, the bridge (603) receives the broadcast feed (601), which includes the EMM (615), ECM (613) and CA protected content (611). The bridge (603) provides the EMM

(627) and ECM (625) to the secondary CA server (609), which has the user key (621). The secondary CA server (609) recovers the control word (641) for descrambling the content. The secondary CA server provides the DRM protected control word to the authorized bridge (603) through a network connection. The authorized bridge descrambles the content and stores the content in the storage (605). The recorded content (643) in the storage (605) is protected using a DRM system. Only the renderer (607) with the appropriate rights (623) can use the recorded content (643). In one embodiment of the present invention, the rights to the recorded content (643) are derived from the entitlement management message and the entitlement control message of the CA system of the primary security system. In one embodiment, the rights are derived from the messages at the time of recording. In one embodiment of the present invention, the rights may be further changed according to subsequent entitlement management messages.

[00113] In one embodiment, the bridge (603) is combined with renderer (607), which can play back the media content in real time. Since the control word is provided through the network, unpredictable network delay may cause glitches in synchronizing the control word with the media stream. In one embodiment of the present invention, the bridge buffers a time period of media stream so that the network delay does not interrupt the continuous playback of the media stream.

[00114] In one embodiment of the present invention, a system can automatically switch between removing the CA protection at the time of recording and removing the CA protection at the time of playing back. For example, the system may automatically remove the CA protection at the time of recording for the content that

the user is entitled to use at the time of recording and remove the CA protection at the time of playing back for the content that the user is not entitled to use at the time of recording. Alternatively, the switching may be based on a user preference, or based on the capability of the components used on the system (e.g., whether or not a bridge has a standard descrambler, or whether or not renderer has a standard descrambler), or partially based on the data in an entitlement management message.

[00115] **Figure 13** illustrates a system in which a secondary CA server is configured to automatically decode the control words before capturing media content into a storage device, or after retrieving captured media content from the storage device, according to one embodiment of the present invention. In **Figure 13**, the bridge (603) receives the broadcast (601), which includes the EMM (615), ECM (613) and CA protected content (611). The bridge (603) provides the EMM (627) and ECM (625) to the secondary CA server (609), which has the user key (621). For the content that the user is entitled to use at the time of recording, the secondary CA server (609) extracts the control word (641) from the ECM (625) and EMM (627) for the bridge (603). The bridge (603) can then descramble the content. After the CA protection is removed, the content (643) in the storage (605) is placed in a DRM system to prevent unauthorized use. If the CA protection for the content is to be removed at the time of playback, the scrambled content and the ECM (617) are stored in the storage (605), protected by the DRM system. Alternatively, the secondary CA server (609) may manage the service keys for the decryption of the entitlement control message at a later time. After retrieving the CA protected content, if the CA protection is not already removed, the renderer (607) sends the

ECM (625) to the secondary CA server (609) protected by the DRM system, which releases the control word (619) only to a renderer (607) with the appropriate rights (623).

[00116] In one embodiment of the present invention, a system according to the present invention performs a CA translation so that the condition access protection for a recorded content is more suitable for the protection of content stored on a storage.

[00117] **Figure 14** illustrates a system in which a secondary CA server is configured to generate substitutive entitlement control messages and decode the control words for the captured media content retrieved from a storage device according to one embodiment of the present invention. In **Figure 14**, the bridge (603) receives the broadcast (601), which includes the EMM (615), ECM_a (613) and CA protected content (611). The bridge (603) provides the EMM (627) and ECM_a (625) to the secondary CA server (609), which has the user key (621). The secondary CA server (609) decrypts the ECM_a (625) and generates the local ECM_b (651). The local ECM_b (651) is provided as a substitutive entitlement control message to replace the original entitlement control message for recording. Typically only the secondary CA server (609) can decrypt the local ECM_b (651). For example, the secondary CA server (609) may generate a unique service key to create local entitlement control message; alternatively, the secondary CA server (609) may encrypt the entitlement control message so that the local entitlement control message can only be decrypted using the user key (621). The local entitlement control message replaces the original entitlement control message; and the local entitlement

control message and the scrambled contents are recorded in the storage (605). The recorded data (653) in the storage (605) may be optionally protected using a DRM system. To use the recorded content, the renderer (607) sends the local entitlement control message (655) back to the secondary CA server (609) protected by the DRM system to get in return the control word (619). To prevent unauthorized access, the secondary CA server provides the control word (619) under the protection of a DRM system so that only the renderer (607) with the appropriate rights (623) can used the control word (619).

[00118] In one embodiment of the present invention, a substitutive entitlement control message contains a control word that is different from the original control word in the original entitlement control message. In addition to sending the substitutive entitlement control message to the bridge (603), the secondary conditional server (609) also sends the original and the substitutive control words to the bridge (603), under the protection of a DRM system. The bridge (603) then descrambles the content using the original control word, re-scrambles the content using the substitutive control word, and replaces the original entitlement control message with the substitutive entitlement control message for recording. In one embodiment of the present invention, the CA protection is translated so that the CA protection for the recorded content is suitable for the management of playing back. For example, an entire recorded movie may be re-scrambled using one same control word so that only one control word is need to play the entire recorded movie. In one embodiment of the present invention, the bridge and the secondary CA server are combined in one; thus, the secondary CA server can performed the task of the

descrambling/re-scrambling. Alternatively, the bridge may send the content to the secondary condition access server through a network connection for the descrambling/re-scrambling task, which may increase the network traffic substantially.

[00119] **Figure 15** shows a method of using a secondary CA server according to one embodiment of the present invention. Operation 701 receives, at a secondary CA server, entitlement management messages of a primary security system (e.g., digital cable television, or satellite television, or a digital radio broadcast system). The entitlement management messages may be directly received from the primary security system, or indirectly received from a bridge through a network connection.. Operation 703 processes the entitlement management messages on the secondary CA server. The secondary CA server has data (e.g., a user key) representing the subscriber, which is used to access data in the entitlement management messages. Operation 705 transmits access controlled data that is in an access controlled format and that is at least partially derived from the entitlement management messages from the secondary CA server to a secondary CA client through a network connection. Operation 707 receives the access controlled data at the secondary CA client from the secondary CA server through the network connection. The access controlled data can be entitlement (such as a service key) extracted from the entitlement management messages, control word, a decrypted entitlement control message (e.g., for an entitlement control message received directly from the primary security system, indirectly from a bridge across a network connection, or retrieved from a storage), a substitutive entitlement control message, control word descrambled

content, control word rescrambled content, etc.

[00120] **Figure 16** shows a detailed method of a secondary CA server according to one embodiment of the present invention. In one embodiment of the present invention, a secondary CA server can provide services to various different clients according to the requests received from the secondary CA clients. Operation 801 determines if an entitlement management message (EMM) is received. If an EMM is received (e.g., from a network bridge, or directly from the broadcast), operation 803 processes the EMM; and operation 805 determines the rights of secondary CA clients according to the data in the EMM. For example, the secondary CA server can extract the entitlement (such as the service key). Operation 807 determines if a request for data is received from a secondary CA client. If a request for data is received, operation 809 determines if the client is entitled to use the data.

[00121] In one embodiment of the present invention, a network bridge may record the content even if the subscriber is not entitled to use the content at the time of recording, since the subscriber may obtain the authorization to use the recorded content after the content is recorded. The network bridge may request a substitutive ECM even if the bridge is not entitled to use. The substitutive ECM is encrypted so that the network bridge cannot obtain the control word from the substitutive ECM. The network bridge can replace the original ECM with the substitutive ECM for recording so that when the subscriber later obtains the authorization to play back the content, the secondary CA server can decrypt the substitutive ECM.

[00122] In one embodiment, if operation 809 determines the client is not entitled to use the data and operation 811 determines the request is not for a substitutive

ECM, access to the data is denied in operation 813. If the request is for a substitutive ECM, operation 815 determines if the decryption key for the ECM is available. In one embodiment of the present invention, a CA system may or may allow the recording of certain content. Thus, the secondary conditional server may or may not have the decryption key for the ECM. If the decryption is not available, operation 813 denies the access; otherwise, operation 817 generates a substitutive ECM through decrypting the original ECM and re-encrypting the ECM so that the substitutive ECM can be later decrypted using a key available to the secondary CA server. Operation 819 then sends the substitutive ECM to the secondary CA client.

[00123] If operation 809 determines the client is entitled to use the data, operation 825 determines if an ECM is received for processing. An ECM may be received from a secondary CA client (e.g., from a bridge that obtains the ECM from the broadcast, or from a renderer that obtains the ECM from a storage for recorded media content) or directly from the broadcast. If an ECM is received for processing, operation 827 determines the decryption key of the ECM. The decryption key may be derived from a recently received EMM, or from the data maintained by the secondary CA server for recorded content. The decryption key can be used to access the control word in the ECM. If operation 827 determines that the request is for the control word, operation 831 sends the control word to the secondary CA client. The control word can be sent in a similar way for sending the service key to prevent unauthorized use. Other data, such as descrambled content, can also be sent in a similar way.

[00124] If operation 829 determines the request is not for the control word and

operation 833 determines the request is for a substitutive ECM, operation 835 determines if rescrambling is required. If rescrambling is required, operation 837 obtains a new control word; and operation 839 sends both the original and the new control words to the secondary CA client. Operation 841 generates a substitutive ECM. The substitutive ECM has the new control word if rescrambling is required; otherwise, the substitutive ECM contains the original control word. Operation 843 then sends the substitutive ECM to the secondary CA client.

[00125] If operation 845 determines the request is for content, operation 849 determines whether the scrambled content is received. If the content is not received, operation 851 retrieves the content from a storage. In one embodiment of the present invention, the secondary CA server has a storage to record the scrambled content. Then, the secondary CA server processes the scrambled content.

[00126] If operation 853 determines descrambling is required, operation 855 control word descrambles the content using the control word in the ECM associated with the content. If operation 857 determines that rescrambling is required, operation 859 control word rescrambles the content using a new control word. If operation 861 determines that the request is for recording the content, operation 865 stores the content; otherwise, operation 863 sends the content to the secondary CA client.

[00127] If operation 845 determines the request is for the content, operation 847 further processes request. For example, the client may request the entitlement information, available contents recorded on a storage, rights to play back or record, or others.

[00128] It is understood that **Figure 16** illustrates an example flow chart of the

operations in a secondary CA server according to one embodiment of the present invention. Some implementations of secondary CA servers may include more or less operations. And the operation sequences are illustrative. From this description, one person skilled in the art understands that many variations and combinations can be implemented.

[00129] In one embodiment of the present invention, various components, such as a bridge, a renderer, a secondary CA server, a storage, or various different combinations of these components, can be implemented using a digital data processing system, such as a computer.

[00130] **Figure 1** shows one example of a typical computer system which may be used with the present invention. Note that while **Figure 1** illustrates various components of a computer system, it is not intended to represent any particular architecture or manner of interconnecting the components as such details are not germane to the present invention. It will also be appreciated that network computers and other data processing systems which have fewer or more components may also be used with the present invention. The computer system of **Figure 1** may, for example, be a Sun workstation, or a personal computer (PC) running a Windows operating system, or an Apple Macintosh computer, or a set top box, or other media controller.

[00131] As shown in **Figure 1**, the computer system 101, which is a form of a data processing system, includes a bus 102 and system core logic 112 which interconnect a microprocessor 103, a ROM 107, and volatile RAM 105 and a non-volatile memory 106. The microprocessor 103, which may be, for example, a G3 or

G4 or G5 microprocessor from Motorola, Inc. or IBM is coupled to cache memory 104 as shown in the example of **Figure 1**. The bus 102 and system core logic 112 interconnect these various components together and also interconnects these components 103, 107, 105, and 106 to a display controller and display device 108 and to peripheral devices such as input/output (I/O) devices which may be mice, keyboards, modems, network interfaces, printers, scanners, video cameras and other devices which are well known in the art. Typically, the input/output devices 110 are coupled to the system through input/output controllers 109. The volatile RAM 105 is typically implemented as dynamic RAM (DRAM) which requires power continually in order to refresh or maintain the data in the memory. The non-volatile memory 106 is typically a magnetic hard drive, a magnetic optical drive, or an optical drive (e.g., a DVD RAM), or other type of memory system which maintains data even after power is removed from the system. Typically, the non-volatile memory will also be a random access memory although this is not required. While **Figure 1** shows that the non-volatile memory is a local device coupled directly to the rest of the components in the data processing system, it will be appreciated that the present invention may utilize a non-volatile memory which is remote from the system, such as a network storage device that is coupled to the data processing system through a network interface such as a modem or Ethernet interface. The bus 102 may include one or more buses connected to one another through various bridges, controllers and/or adapters as is well known in the art. In one embodiment the I/O controller 109 includes a USB (Universal Serial Bus) adapter for controlling USB peripherals, and/or an IEEE-1394 bus adapter for controlling IEEE-1394 peripherals.

[00132] It will be apparent from this description that aspects of the present invention may be embodied, at least in part, in software. That is, the techniques may be carried out in a computer system or other data processing system in response to its processor, such as a microprocessor, executing sequences of instructions contained in a memory, such as ROM 107, volatile RAM 105, non-volatile memory 106, cache 104 or a remote storage device. In various embodiments, hardwired circuitry may be used in combination with software instructions to implement the present invention. Thus, the techniques are not limited to any specific combination of hardware circuitry and software nor to any particular source for the instructions executed by the data processing system. In addition, throughout this description, various functions and operations are described as being performed by or caused by software code to simplify description. However, those skilled in the art will recognize what is meant by such expressions is that the functions result from execution of the code by a processor, such as the microprocessor 103.

[00133] A machine readable medium can be used to store software and data which when executed by a data processing system causes the system to perform various methods of the present invention. This executable software and data may be stored in various places including for example ROM 107, volatile RAM 105, non-volatile memory 106 and/or cache 104 as shown in **Figure 1**. Portions of this software and/or data may be stored in any one of these storage devices.

[00134] Thus, a machine readable medium includes any mechanism that provides (i.e., stores and/or transmits) information in a form accessible by a machine (e.g., a computer, network device, personal digital assistant, manufacturing tool, any device

IPR2025-00305
ASUS EX1002 Page 62

with a set of one or more processors, etc.). For example, a machine readable medium includes recordable/non-recordable media (e.g., read only memory (ROM), random access memory (RAM), magnetic disk storage media, optical storage media, flash memory devices, etc.), as well as electrical, optical, acoustical or other forms of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.), etc.

[00135] In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will be evident that various modifications may be made thereto without departing from the broader spirit and scope of the invention as set forth in the following claims. The specification and drawings are, accordingly, to be regarded in an illustrative sense rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method to control a presentation of content, the method comprising:

receiving a representation of content from a first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access; and

presenting the content, at a user's request, through a second conditional access server which is coupled to the first conditional access server;

wherein the presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively; and

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content.

2. The method of claim 1, wherein the content is presented by a network client of the second conditional access server using the second set of cryptographic keys.

IPR2025-00305
ASUS EX1002 Page 64

3. The method of claim 2, wherein the first conditional access server provides the second conditional access server the first set of cryptographic keys for authorized use.

4. The method of claim 3, wherein the user's request is after the first conditional access server provides at least a portion of the content; and the portion of the content is presented in response to the user's request.

5. The method of claim 2, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the network client is a digital rights management client.

6. The method of claim 5, wherein the second conditional access server authorizes the network client to use the content through the digital rights management system in accordance with authorization to use received from the first conditional access server.

7. The method of claim 1, wherein the second conditional access server translates authorization to access the content from authorization received from the first conditional access server to authorization for the network client.

8. The method of claim 1, wherein the second set of cryptographic keys consists one key.

9. The method of claim 1, wherein the second conditional access server acts as a primary conditional access server to another secondary conditional access server.

10. A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content, the method comprising:

receiving, at a second conditional access server, a first set of cryptographic keys from a first conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys; and

authorizing a client of the second conditional access server to present the content in accordance with authorization the second conditional access server received from the first conditional access server;

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content.

11. The medium of claim 10, wherein the method further comprises:
recording a representation of the content in an encrypted form in response to a message from the first conditional access server.

12. The medium of claim 11, wherein the client sends a request, through a network connection to the second conditional access server, for authorization to present the content after the first conditional access server provides at least a portion of the content which is recorded; and the second conditional access server obtains authorization from the first conditional access server, after the first conditional access server provides the portion of the content, for said authorizing.

13. The medium of claim 10, wherein the method further comprises:
translating authorization to access the content from authorization received from the first conditional access server to authorization for the client.

14. The medium of claim 13, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the client comprises a digital rights management client.

15. The medium of claim 14, wherein the second conditional access server authorizes the client to use the content through the digital rights management

system in accordance with authorization received from the first conditional access server.

16. The medium of claim 15, wherein the first conditional access server provides authorization to the second conditional access server according to an identity of the second conditional access server; the second conditional access server provides authorization to the client according to an identity of the client; and the first conditional access server is not aware of an identity of the client.

17. The medium of claim 10, wherein the second set of cryptographic keys consists one key.

18. The medium of claim 10, wherein the second conditional access server is a server of a further secondary conditional access server and acts as a primary conditional access server with respect to the further secondary conditional access server.

19. A secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

a communication interface, the communication interface to receive a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and

authorizes access to the content through the first set of cryptographic keys; and

a controller coupled to the communication interface, the controller to authorize a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server;

wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content.

20. The secondary conditional access server of claim 19, wherein the controller is to translate authorization to access the content from authorization received from the primary conditional access server to authorization for the client.

21. The secondary conditional access server of claim 20, wherein the second set of cryptographic keys comprises a key of a digital rights management system; the client comprises a digital rights management client; and the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server.

22. The secondary conditional access server of claim 20, wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of the client; and the primary conditional access server is not aware of an identity of the client.

23. A secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

means for receiving a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys; and

means for authorizing a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server;

wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content.

24. The secondary conditional access server of claim 23, further comprising:

means for recording a representation of the content in an encrypted form in response to a message from the primary conditional access server.

wherein the client sends a request, through a network connection to the secondary conditional access server, for authorization to present the content after the primary conditional access server provides at least a portion of the content which is recorded; and

the secondary conditional access server obtains authorization from the primary conditional access server, after the primary conditional access server provides the portion of the content, for authorizing the client to present the content.

25. The secondary conditional access server of claim 23, further comprising:

means for translating authorization to access the content from authorization received from the primary conditional access server to authorization for the client.

wherein the second set of cryptographic keys comprises a key of a digital rights management system; and

the client comprises a digital rights management client; and

wherein the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server.

26. The secondary conditional access server of claim 23, wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of the client; and the primary conditional access server is not aware of an identity of the client.

27. The secondary conditional access server of claim 23, wherein the second set of cryptographic keys consists one key.

28. A method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component;

broadcasting the media component from a first conditional access server;

receiving a client request to use the media component from a client through a second conditional access server after said broadcasting; and

responding to the client request through the second conditional access server.

29. The method of claim 28, further comprising:

broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

30. The method of claim 29, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

31. The method of claim 30, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

32. A method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system;

processing the security messages on the conditional access server; and

transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages.

33. The method of claim 32, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system.

34. The method of claim 32, wherein the access controlled data is protected using a digital rights management system.

35. The method of claim 34, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

36. The method of claim 34, further comprising:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

37. The method of claim 36, wherein the access controlled data comprises a decrypted version of the entitlement control message.

38. The method of claim 34, further comprising:

receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

39. The method of claim 38, further comprising:

storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

40. The method of claim 32, further comprising:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

41. The method of claim 40, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

42. The method of claim 41, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

43. The method of claim 41, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

44. The method of claim 41, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

45. The method of claim 44, wherein the access controlled data further comprises the first and second control words.

46. The method of claim 32, further comprising:

receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

generating a second entitlement control message containing a second control word that is different from the first control word; and

descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

47. The method of claim 46, further comprising:

storing, at the conditional access server, the content rescrambled by the second control word; and

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

48. A method to process media content provided by a primary security system, the method comprising:

receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system.

49. The method of claim 48, wherein the security message is an entitlement message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

50. The method of claim 48, wherein the access controlled format protects access to data using a digital rights management system.

51. The method of claim 50, further comprising:

automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

descrambling and recording the portion of the media content in response to a determination to descramble; and

recording the portion of the media content without descrambling in response to a determination not to descramble.

52. The method of claim 50, further comprising:

sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

53. The method of claim 52, further comprising:

descrambling media content using the control word; and

storing the media content in a storage under protection of a digital rights management system.

54. The method of claim 52, further comprising:

descrambling media content using the control word; and

rendering the media content for presentation.

55. The method of claim 54, further comprising:

retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

56. The method of claim 52, wherein the access controlled data comprises a decrypted version of the entitlement control message.

57. The method of claim 50, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

58. The method of claim 48, further comprising:

receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

59. The method of claim 58, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the method further comprises:
storing the second entitlement control message with the portion of the media content.

60. The method of claim 59, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

61. The method of claim 59, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further comprises:
descrambling the content using the first control word and rescrambling the content using the second control word.

62. A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component;

broadcasting the media component from a first conditional access server;

receiving a client request to use the media component from a client through a second conditional access server after said broadcasting; and

responding to the client request through the second conditional access server.

63. The medium of claim 62, wherein the method further comprises:

broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

64. The medium of claim 63, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

65. The medium of claim 64, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the

media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

66. A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system;

processing the security messages on the conditional access server; and

transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages.

67. The medium of claim 66, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system.

68. The medium of claim 66, wherein the access controlled data is protected using a digital rights management system.

69. The medium of claim 68, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

70. The medium of claim 68, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

71. The medium of claim 70, wherein the access controlled data comprises a decrypted version of the entitlement control message.

72. The medium of claim 68, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

73. The medium of claim 72, wherein the method further comprises:

storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

74. The medium of claim 66, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

75. The medium of claim 74, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

76. The medium of claim 75, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

77. The medium of claim 75, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

78. The medium of claim 75, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

79. The medium of claim 78, wherein the access controlled data further comprises the first and second control words.

80. The medium of claim 66, wherein the method further comprises:

receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

generating a second entitlement control message containing a second control word that is different from the first control word; and

descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

81. The medium of claim 80, wherein the method further comprises:

storing, at the conditional access server, the content rescrambled by the second control word; and

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

82. A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process media content provided by a primary security system, the method comprising:

receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system.

83. The medium of claim 82, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

84. The medium of claim 82, wherein the access controlled format protects access to data using a digital rights management system.

85. The medium of claim 84, wherein the method further comprises:

automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

descrambling and recording the portion of the media content in response to a determination to descramble; and

recording the portion of the media content without descrambling in response to a determination not to descramble.

86. The medium of claim 84, wherein the method further comprises:

sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

87. The medium of claim 86, wherein the method further comprises:

descrambling media content using the control word; and

storing the media content in a storage under protection of a digital rights management system.

88. The medium of claim 86, wherein the method further comprises:

descrambling media content using the control word; and

rendering the media content for presentation.

89. The medium of claim 88, wherein the method further comprises:

retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

90. The medium of claim 86, wherein the access controlled data comprises a decrypted version of the entitlement control message.

91. The medium of claim 84, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

92. The medium of claim 82, wherein the method further comprises:

receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

93. The medium of claim 92, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the method further comprises:
storing the second entitlement control message with the portion of the media content.

94. The medium of claim 93, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

95. The medium of claim 93, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further comprises:
descrambling the content using the first control word and rescrambling the content using the second control word.

96. A primary security system to provide conditional access, the system comprising:

means for broadcasting a first entitlement management message for a subscriber to request caching of a media component;

means for broadcasting the media component;

means for receiving a client request to use the media component from a client through a secondary conditional access server after said broadcasting; and

means for responding to the client request through the secondary conditional access server.

97. The system of claim 96, further comprising:

means for broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

98. The system of claim 97, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

99. The system of claim 98, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the

media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

100. A data processing system to process conditional access protection, the data processing system comprising:

means for receiving, at a conditional access server, security messages of a primary security system;

means for processing the security messages on the conditional access server; and

means for transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages.

101. The data processing system of claim 100, wherein the security messages comprise entitlement management messags; the conditional access server has a user key representing a subscriber of the primary security system; and said means for processing the entitlement management messages comprises:

means for decrypting to obtain a service key of the primary security system.

102. The data processing system of claim 100, wherein the access controlled data is protected using a digital rights management system.

103. The data processing system of claim 102, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

104. The data processing system of claim 102, further comprising:

means for receiving, at the conditional access server, an entitlement control message of the primary security system; and

means for processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

105. The data processing system of claim 104, wherein the access controlled data comprises a decrypted version of the entitlement control message.

106. The data processing system of claim 102, further comprising:

means for receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

means for descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

107. The data processing system of claim 106, further comprising:

means for storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

108. The data processing system of claim 100, further comprising:

means for receiving, at the conditional access server, an entitlement control message of the primary security system; and

means for processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

109. The data processing system of claim 108, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

110. The data processing system of claim 109, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

111. The data processing system of claim 109, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

112. The data processing system of claim 109, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

113. The data processing system of claim 112, wherein the access controlled data further comprises the first and second control words.

114. The data processing system of claim 100, further comprising:

means for receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

means for generating a second entitlement control message containing a second control word that is different from the first control word; and

means for descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

115. The data processing system of claim 114, further comprising:

means for storing, at the conditional access server, the content rescrambled by the second control word; and

means for retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

116. A data processing system to process media content provided by a primary security system, the data processing system comprising:

means for receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system.

117. The data processing system of claim 116, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

118. The data processing system of claim 116, wherein the access controlled format protects access to data using a digital rights management system.

119. The data processing system of claim 118, further comprising:

means for automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

means for descrambling and recording the portion of the media content in response to a determination to descramble; and

means for recording the portion of the media content without descrambling in response to a determination not to descramble.

120. The data processing system of claim 118, further comprising:

means for sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

121. The data processing system of claim 120, further comprising:

means for descrambling media content using the control word; and

means for storing the media content in a storage under protection of a digital rights management system.

122. The data processing system of claim 120, further comprising:

means for descrambling media content using the control word; and

means for rendering the media content for presentation.

123. The data processing system of claim 122, further comprising:

means for retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

124. The data processing system of claim 120, wherein the access controlled data comprises a decrypted version of the entitlement control message.

125. The data processing system of claim 118, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

126. The data processing system of claim 116, further comprising:

means for receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

means for sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

127. The data processing system of claim 126, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the system further comprises:

means for storing the second entitlement control message with the portion of the media content.

128. The data processing system of claim 127, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

129. The data processing system of claim 127, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the system further comprises:

means for descrambling the content using the first control word and rescrambling the content using the second control word.

130. A conditional access server, comprising:

one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system;

a processor coupled to the one or more communication interfaces, the processor to process the security messages, and the one or more communication interfaces to transmit, to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages.

131. The conditional access server of claim 130, wherein the security messages comprise entitlement management messages; and the access controlled data is protected using a digital rights management system.

132. The conditional access server of claim 131, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

133. The conditional access server of claim 131, wherein the one or more communication interfaces are to receive an entitlement control message of

the primary security system; the processor is to obtain a control word of the primary security system from the entitlement control message; and the access controlled data comprises the control word.

134. The conditional access server of claim 131, wherein the one or more communication interfaces are to receive an entitlement control message and scrambled content of the primary security system; and the conditional access server further comprises:

a descrambler coupled to the processor, the descrambler to descramble the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

135. The conditional access server of claim 134, further comprising:

a storage device coupled to one or more communication interfaces, the storage device to store the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

136. The conditional access server of claim 130, wherein the one or more communication interfaces are to receive entitlement control message of the primary security system; the processor is to to generate a substitutive entitlement control message as a replacement of the entitlement control

IPR2025-00305
ASUS EX1002 Page 100

message; and the access controlled data comprises the substitutive entitlement control message.

137. The conditional access server of claim 136, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

138. The conditional access server of claim 130, wherein the one or more communication interfaces are to receive a first entitlement control message containing a first control word and content scrambled by the first control word; the processor is to generate a second entitlement control message containing a second control word that is different from the first control word; and the conditional access server further comprises:

a transcrambler coupled to the one or more communication interfaces and the processor, the transcrambler to descramble the content using the first control word and rescramble the content using the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

139. The conditional access server of claim 138, further comprising:

a storage device coupled to the transcrambler, the storage device to store the content rescrambled by the second control word.

140. A secondary conditional access client, comprising:

a communication interface to receive, from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system; and

a processor coupled to the communication interface, the processor to process the access controlled data.

141. The client of claim 140, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

142. The client of claim 140, wherein the access controlled format protects access to data using a digital rights management system.

143. The client of claim 142, wherein the processor is to automatically determine whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data; the client further comprises:

a storage device;

a descrambler coupled to the processor and the storage device, in response to a determination to descramble the descrambler to descramble the portion of the media content for storing in the storage device, in response to a determination not to descramble the storage device to record the portion of the media content without descrambling.

144. The client of claim 142, wherein the communication interface is to send, to the conditional access server through a network connection, an entitlement control message containing a control word in an encrypted form; and the access controlled data comprises the control word.

145. The client of claim 144, further comprising:

a storage device;

a descrambler coupled to the processor and the storage device, the descrambler to descramble media content using the control word, the storage device to store the media content under protection of a digital rights management system.

146. The client of claim 140, further comprising:

an physical interface to receive a first entitlement control message for descrambling a portion of media content received from the primary security system; and

IPR2025-00305
ASUS EX1002 Page 103

wherein the communication interface is to send the first entitlement control message to the conditional access server through a network connection.

ABSTRACT OF THE DISCLOSURE

Conditional access to media content of primary security systems on a secondary networked environment. In one embodiment, a conditional access server is used to provide services to secondary CA clients (e.g., a bridge, a renderer, a storage, or their different combinations) through network connections. Containing data representing the subscriber, a conditional access server recovers entitlement data and/or decryption keys of a primary security system for the conditional access protected content, such as service keys and control words, and/or enforces conditional access to the content by secondary CA clients according to the authorization of the primary security system for the secondary CA clients. In one embodiment, a conditional access system provides delayed authorization for use so that the content can be recorded for later use when authorized and broadcasts rights for use on multiple secondary CA clients.

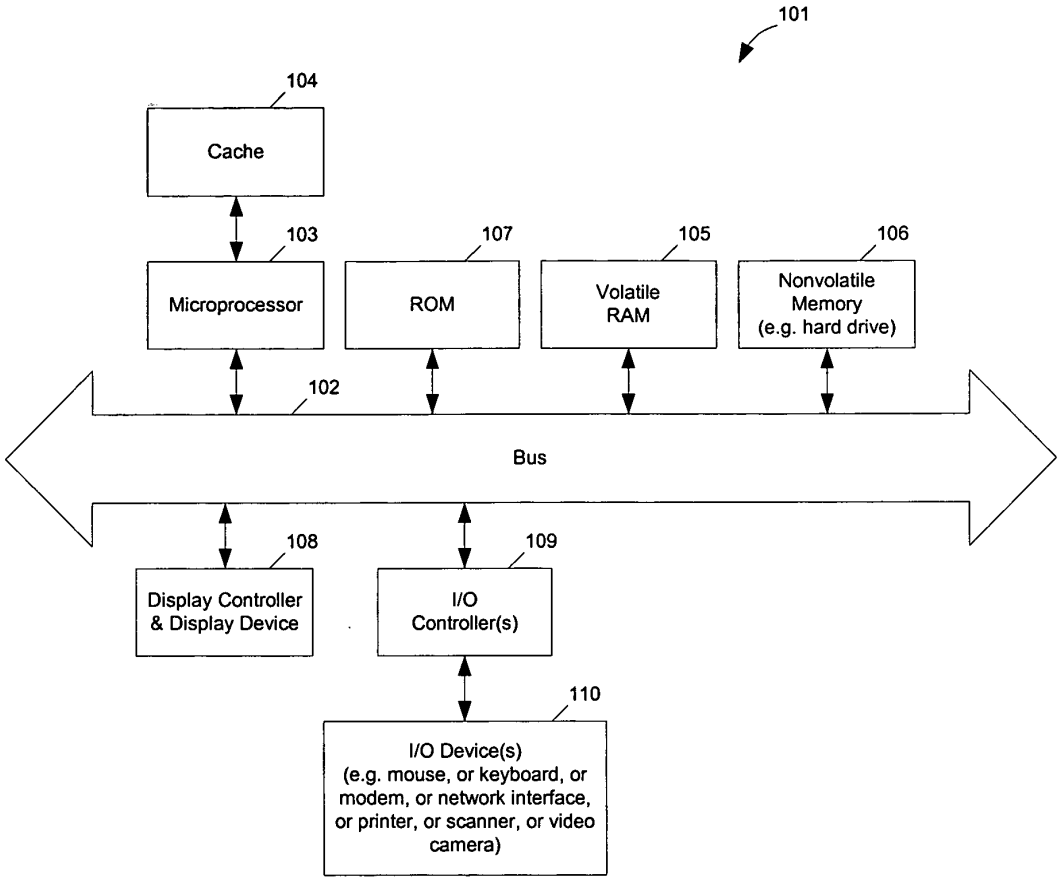

101
104
Cache
103
Microprocessor
107
ROM
105
Volatile RAM
106
Nonvolatile Memory (e.g. hard drive)
102
Bus
108
Display Controller & Display Device
109
I/O Controller(s)
110
I/O Device(s) (e.g. mouse, or keyboard, or modem, or network interface, or printer, or scanner, or video camera)

Fig. 1

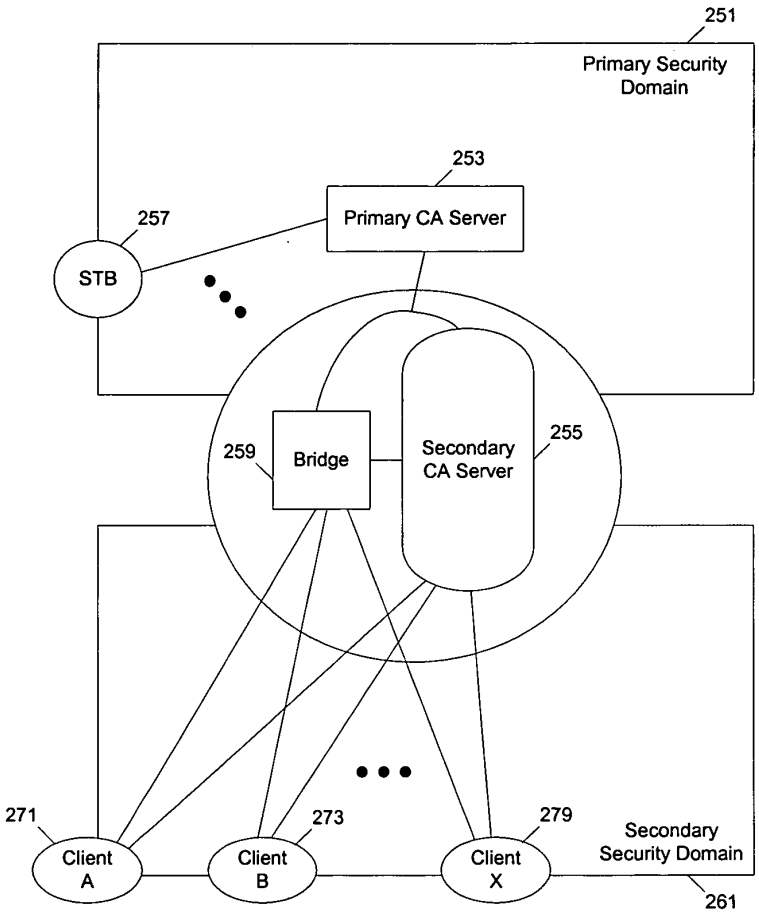

251
Primary Security Domain
253
Primary CA Server
257
STB
259
Bridge
Secondary CA Server
255
271
Client A
273
Client B
279
Client X
Secondary Security Domain
261

Fig. 2A

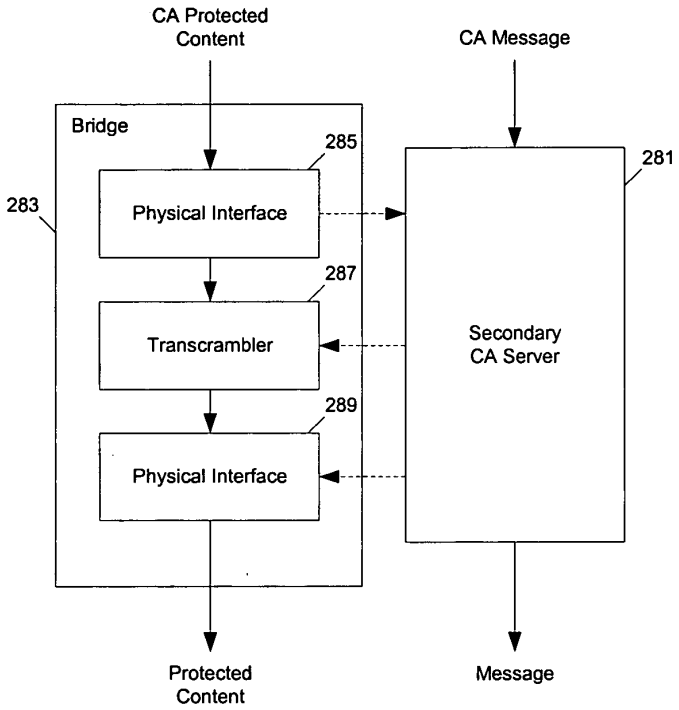

CA Protected Content
CA Message
Bridge
285
281
283
Physical Interface
287
Transcrambler
Secondary CA Server
289
Physical Interface
Protected Content
Message

Fig. 2B

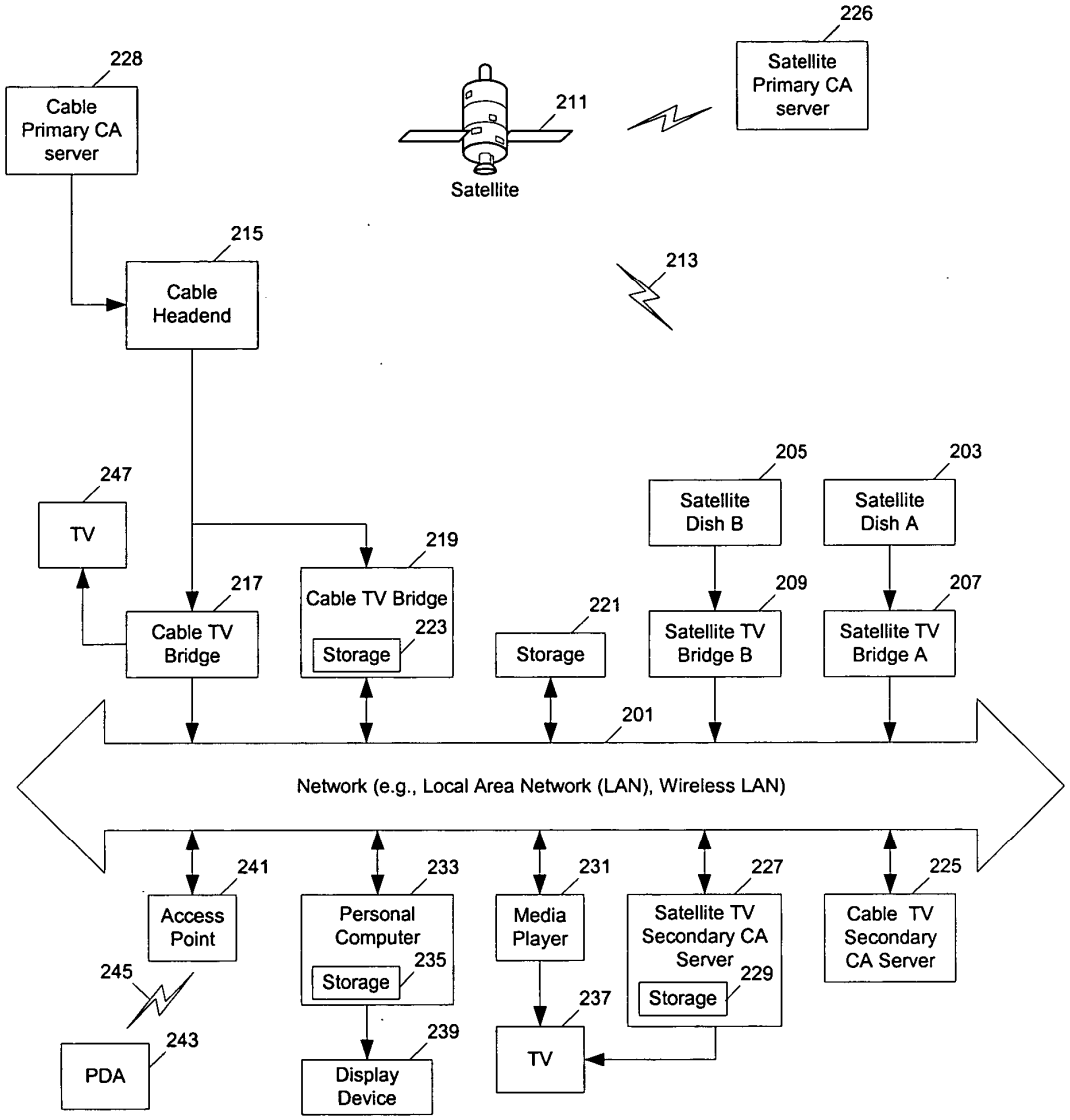

226
Satellite Primary CA server
228
Cable Primary CA server
211
Satellite
215
Cable Headend
213
205
203
247
Satellite Dish B
Satellite Dish A
TV
219
209
207
217
Cable TV Bridge
221
Satellite TV Bridge B
Satellite TV Bridge A
Cable TV Bridge
223
Storage
Storage
201
Network (e.g., Local Area Network (LAN), Wireless LAN)
241
233
231
227
225
Access Point
Personal Computer
Media Player
Satellite TV Secondary CA Server
Cable TV Secondary CA Server
245
235
229
Storage
Storage
237
243
239
PDA
Display Device
TV

Fig. 3

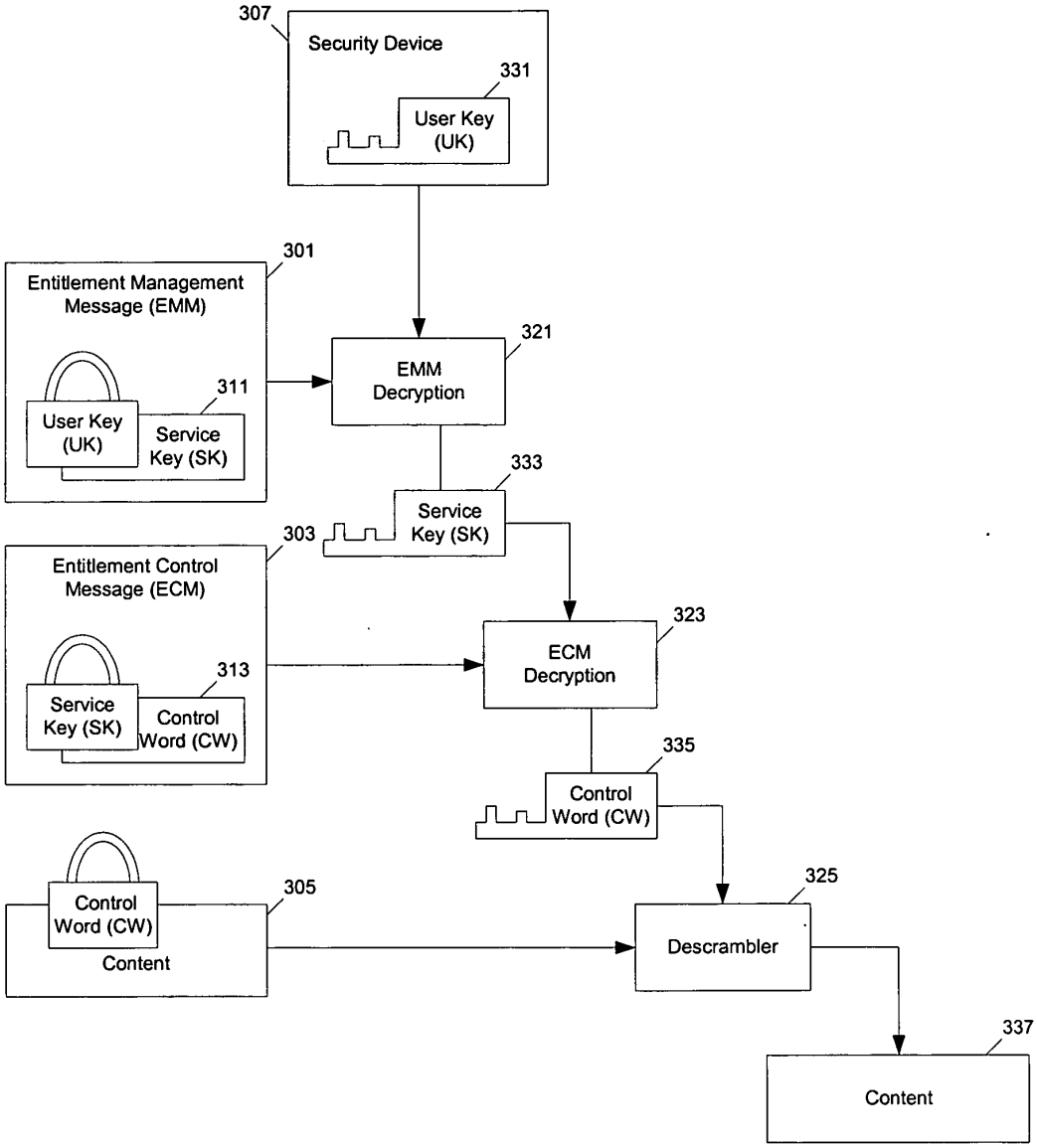

307
Security Device
331
User Key (UK)
301
Entitlement Management Message (EMM)
311
User Key (UK)
Service Key (SK)
321
EMM Decryption
333
Service Key (SK)
303
Entitlement Control Message (ECM)
313
Service Key (SK)
Control Word (CW)
323
ECM Decryption
335
Control Word (CW)
305
Control Word (CW)
Content
325
Descrambler
337
Content

Fig. 4

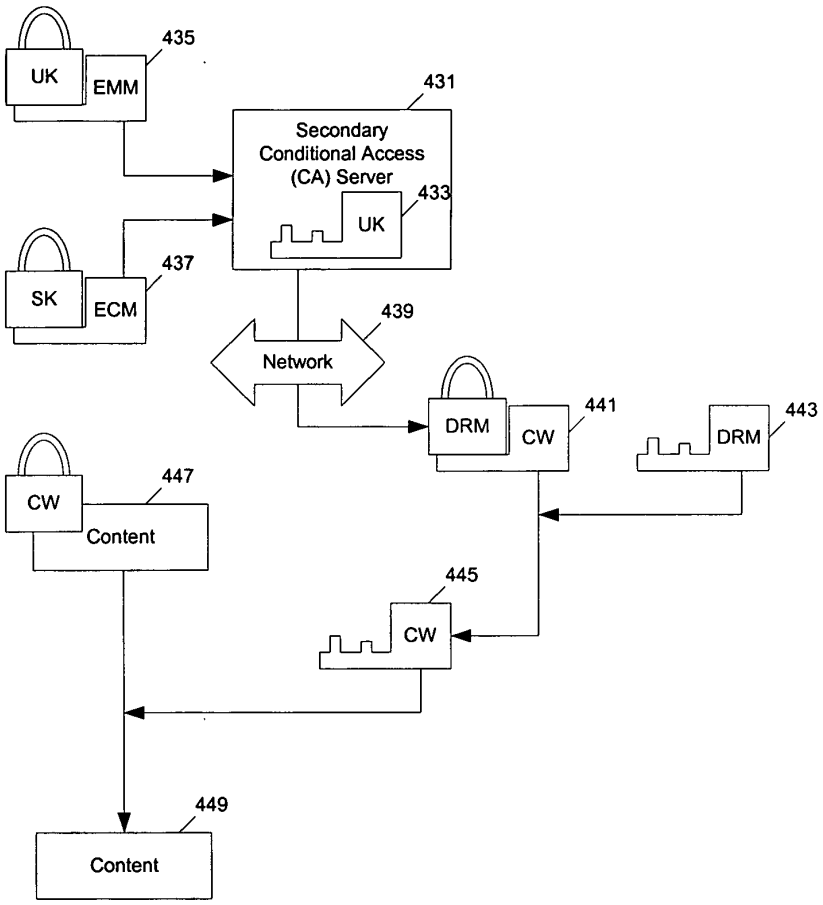

435
UK
EMM
431
Secondary
Conditional Access
(CA) Server
433
UK
437
SK
ECM
439
Network
441
DRM
CW
443
DRM
447
CW
Content
445
CW
449
Content

Fig. 5

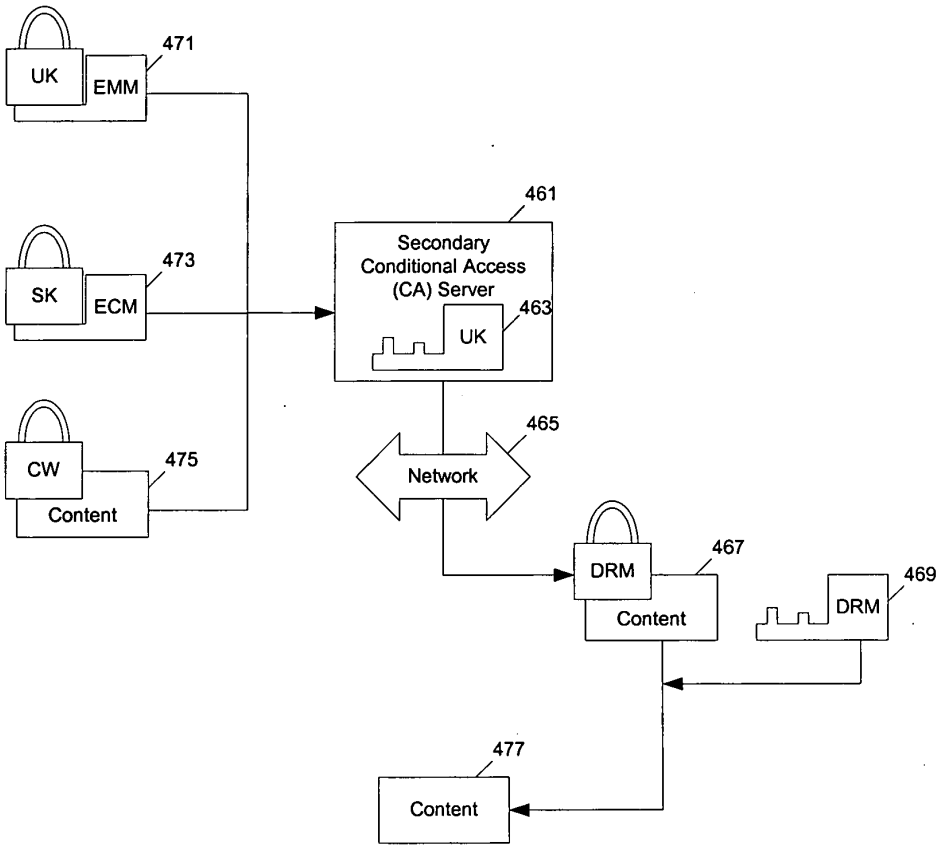

UK
EMM
471
SK
ECM
473
CW
Content
475
461
Secondary
Conditional Access
(CA) Server
UK
463
465
Network
DRM
Content
467
DRM
469
477
Content

Fig. 6

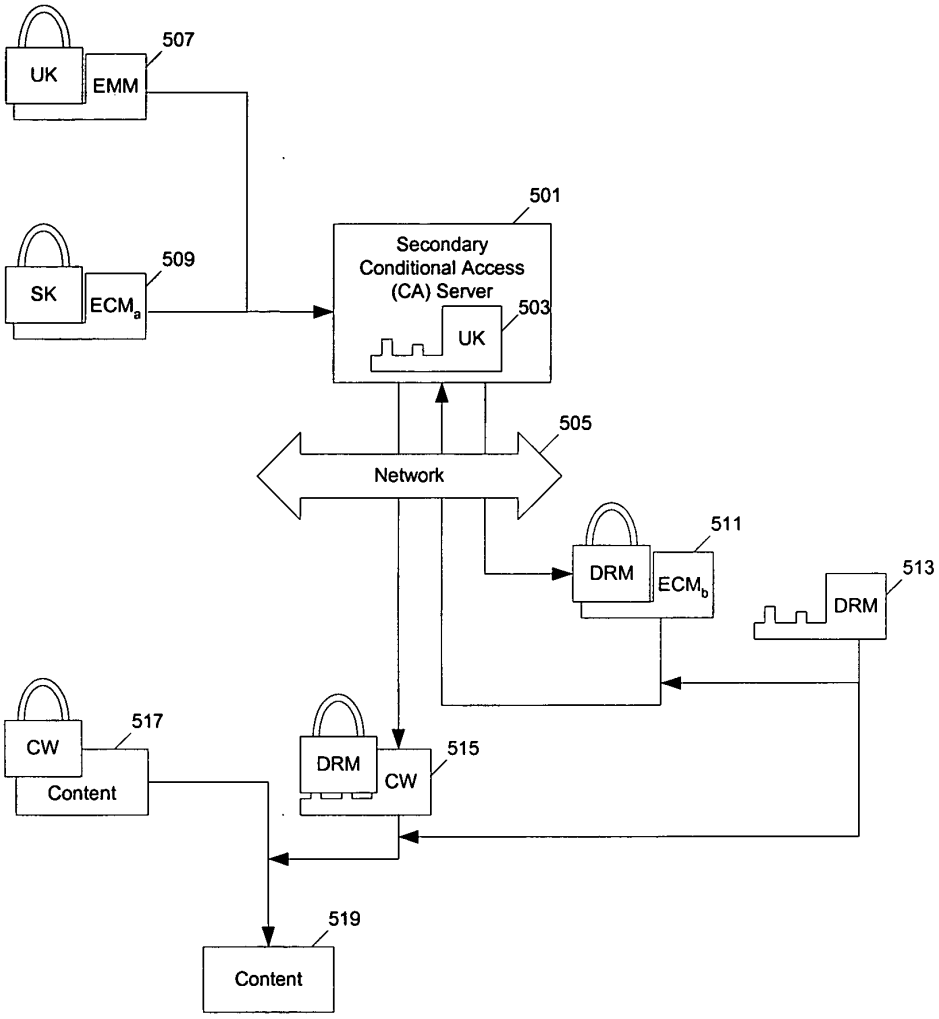

UK
EMM
507
501
SK
ECM_a
509
Secondary
Conditional Access
(CA) Server
503
UK
505
Network
511
DRM
ECM_b
513
DRM
517
CW
Content
DRM
CW
515
519
Content

Fig. 7

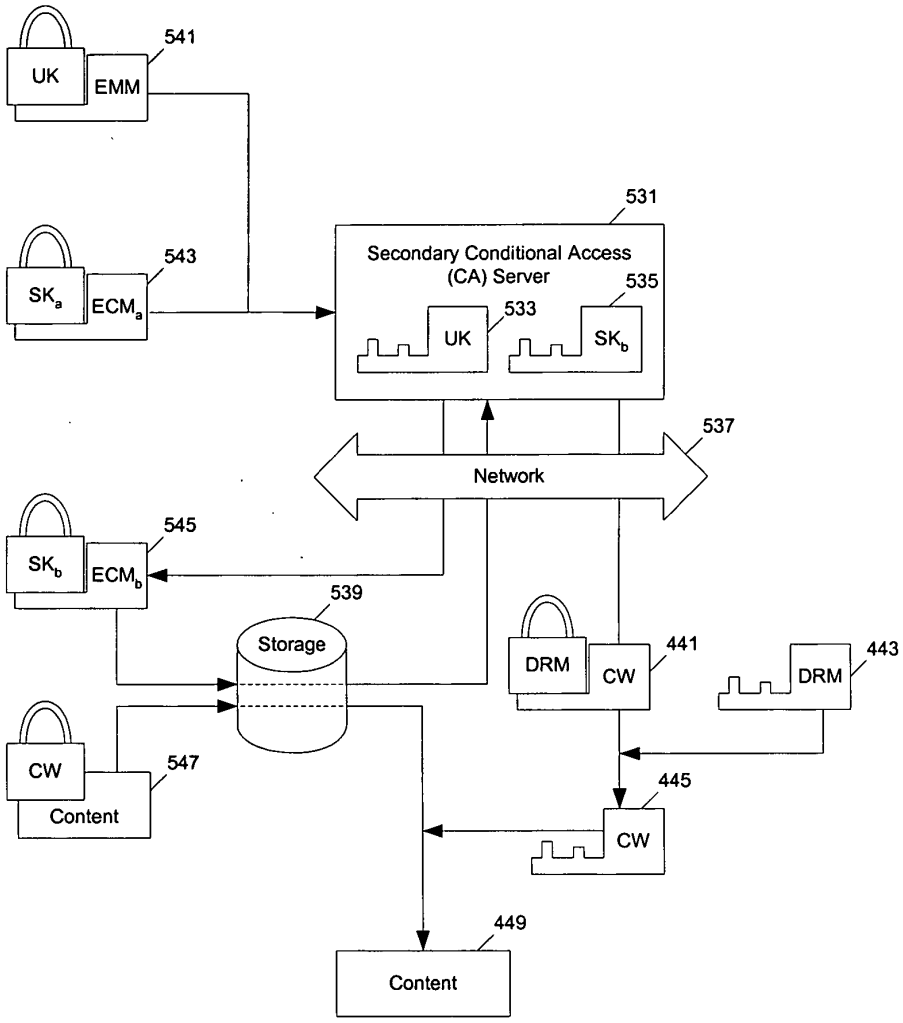

UK
EMM
541
531
Secondary Conditional Access (CA) Server
535
533
UK
SK_b
543
SK_a
ECM_a
537
Network
545
SK_b
ECM_b
539
Storage
DRM
CW
441
DRM
443
CW
Content
547
445
CW
449
Content

Fig. 8

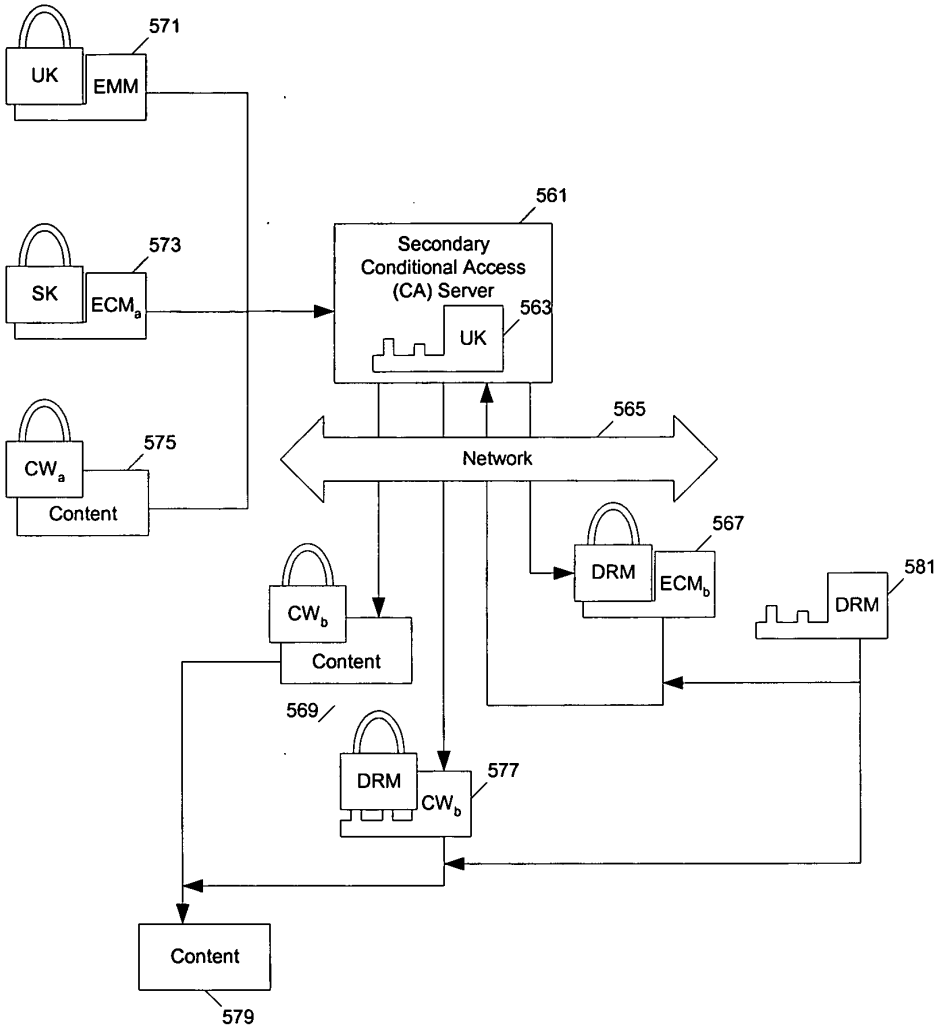

571
UK
EMM
561
Secondary
Conditional Access
(CA) Server
563
UK
573
SK
ECM$_a$
565
Network
575
CW$_a$
Content
567
DRM
ECM$_b$
581
DRM
CW$_b$
Content
569
DRM
CW$_b$
577
Content
579

Fig. 9

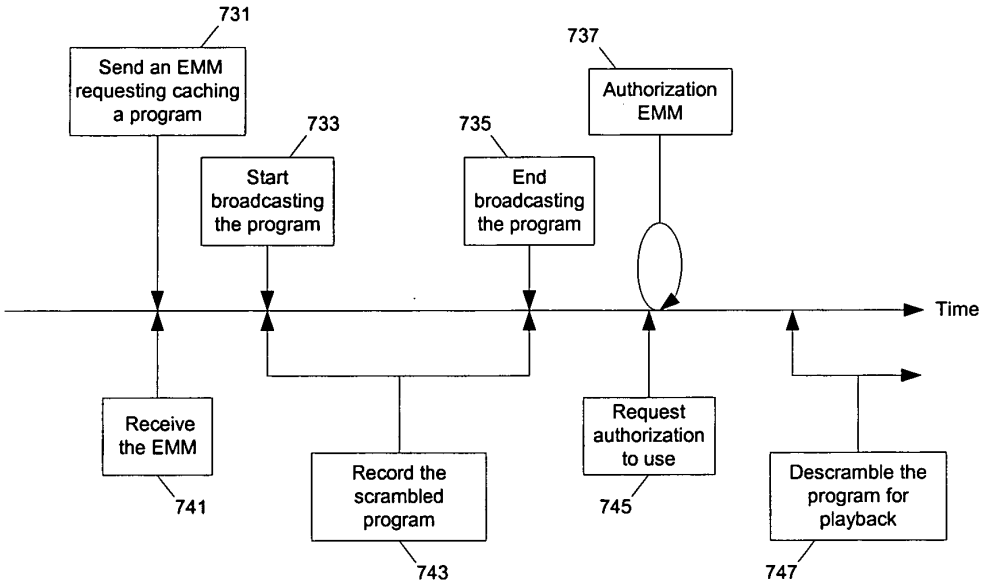
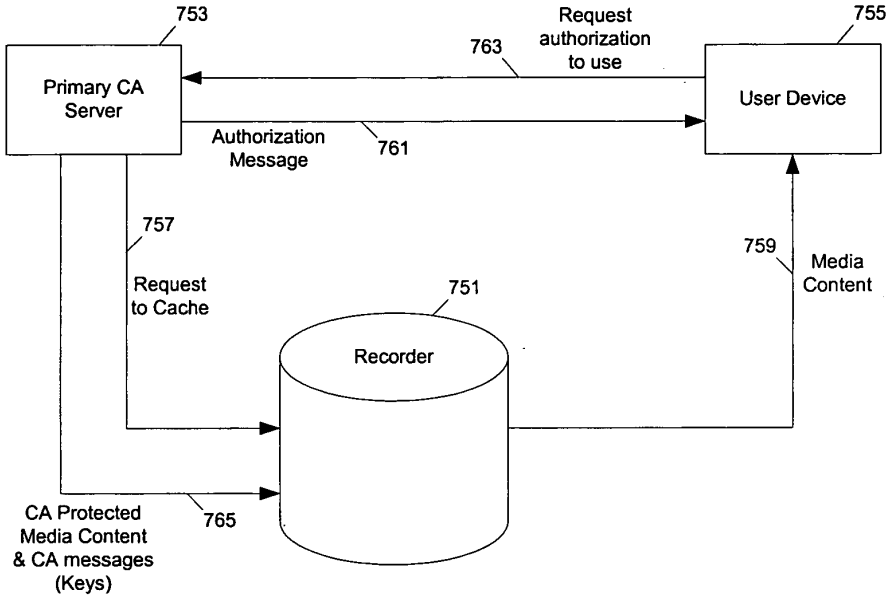

731
Send an EMM requesting caching a program
733
Start broadcasting the program
735
End broadcasting the program
737
Authorization EMM
Time
Receive the EMM
741
Record the scrambled program
743
Request authorization to use
745
Descramble the program for playback
747

Fig. 10A



(Prior Art)

Fig. 10B

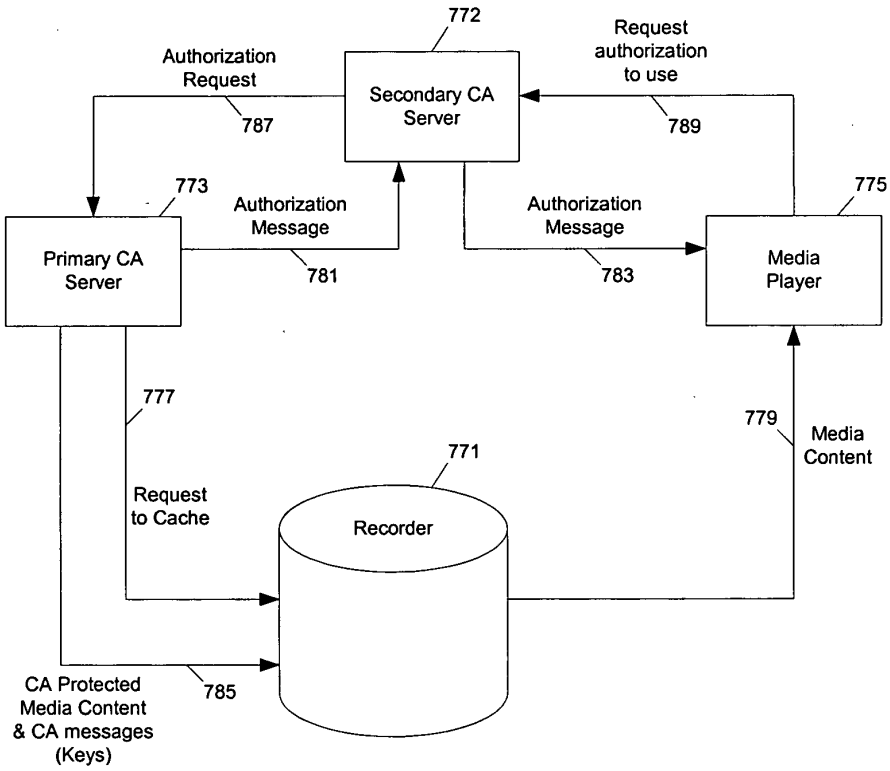

772
Secondary CA Server
Authorization Request
787
Request authorization to use
789
773
Primary CA Server
Authorization Message
781
Authorization Message
783
775
Media Player
777
Request to Cache
771
Recorder
779
Media Content
CA Protected Media Content & CA messages (Keys)
785

Fig. 10C

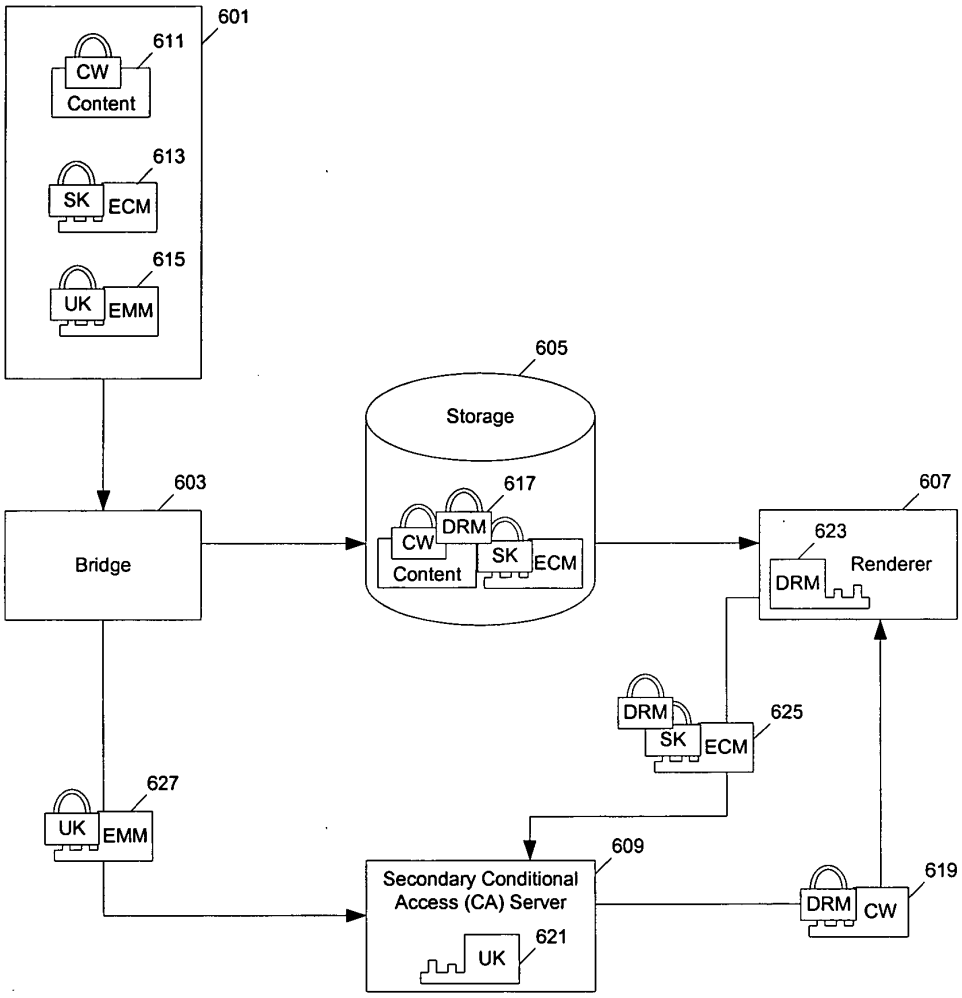

601
611
CW
Content
613
SK
ECM
615
UK
EMM
605
Storage
603
Bridge
617
DRM
CW
Content
SK
ECM
607
623
DRM
Renderer
625
DRM
SK
ECM
627
UK
EMM
609
Secondary Conditional Access (CA) Server
621
UK
619
DRM
CW

Fig. 11

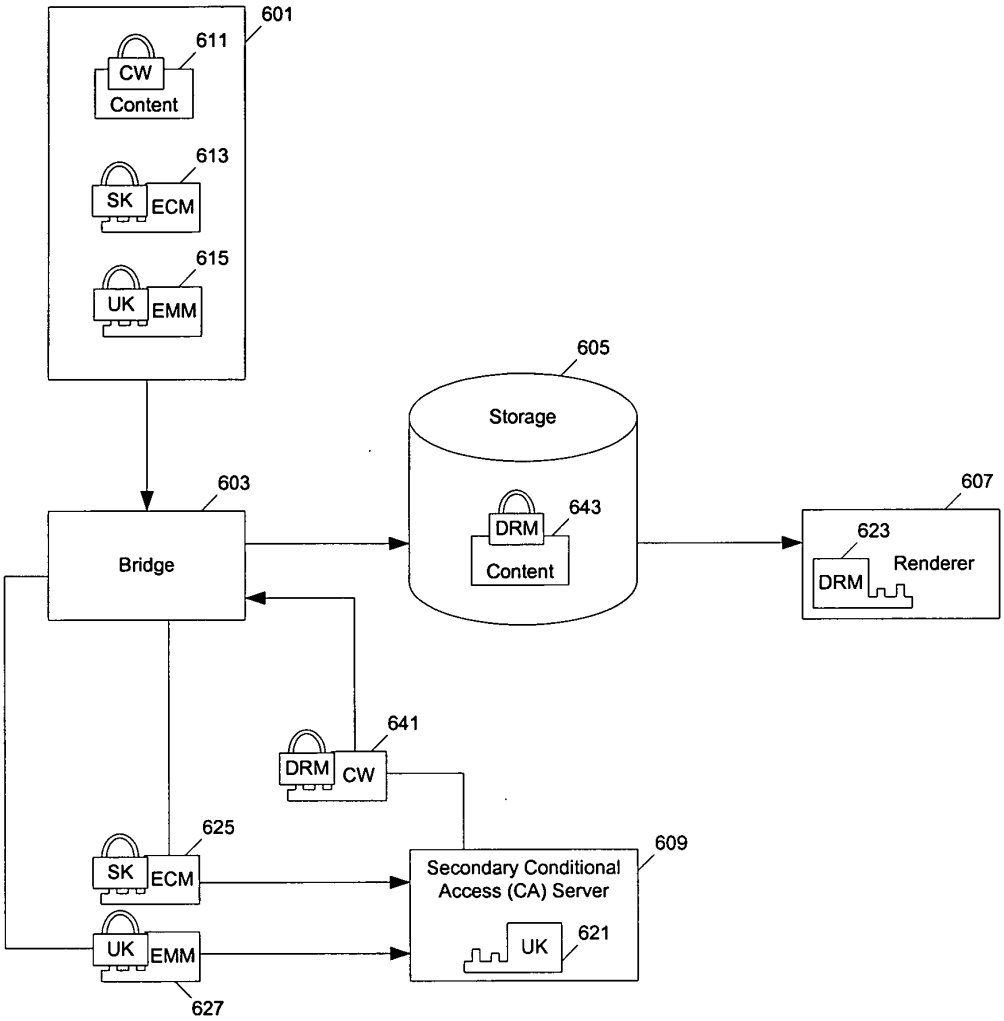

601
611
CW
Content
613
SK
ECM
615
UK
EMM
605
Storage
643
DRM
Content
607
623
DRM
Renderer
603
Bridge
641
DRM
CW
625
SK
ECM
609
Secondary Conditional Access (CA) Server
621
UK
UK
EMM
627

Fig. 12

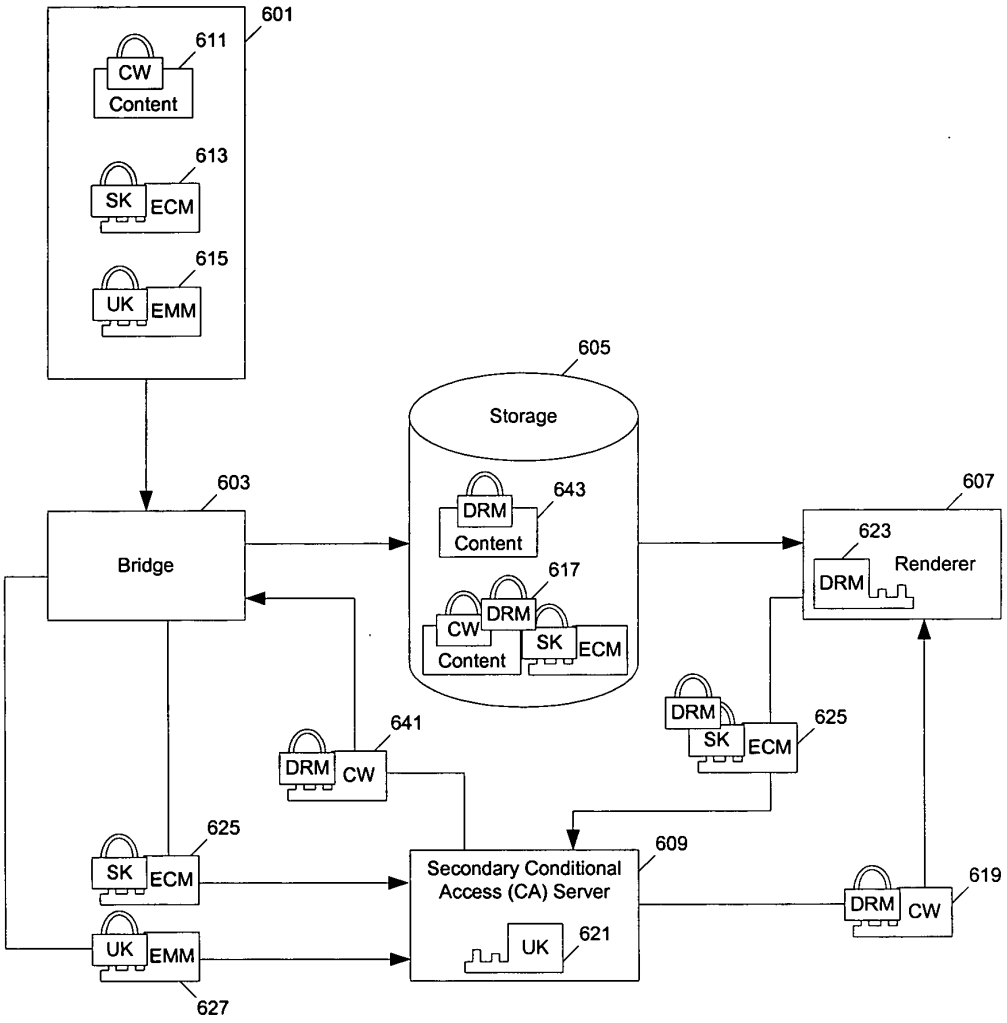

601
611
CW
Content
613
SK
ECM
615
UK
EMM
605
Storage
643
DRM
Content
617
DRM
CW
Content
SK
ECM
603
Bridge
607
623
Renderer
DRM
641
DRM
CW
625
DRM
SK
ECM
625
SK
ECM
609
Secondary Conditional Access (CA) Server
UK
621
UK
EMM
627
619
DRM
CW

Fig. 13

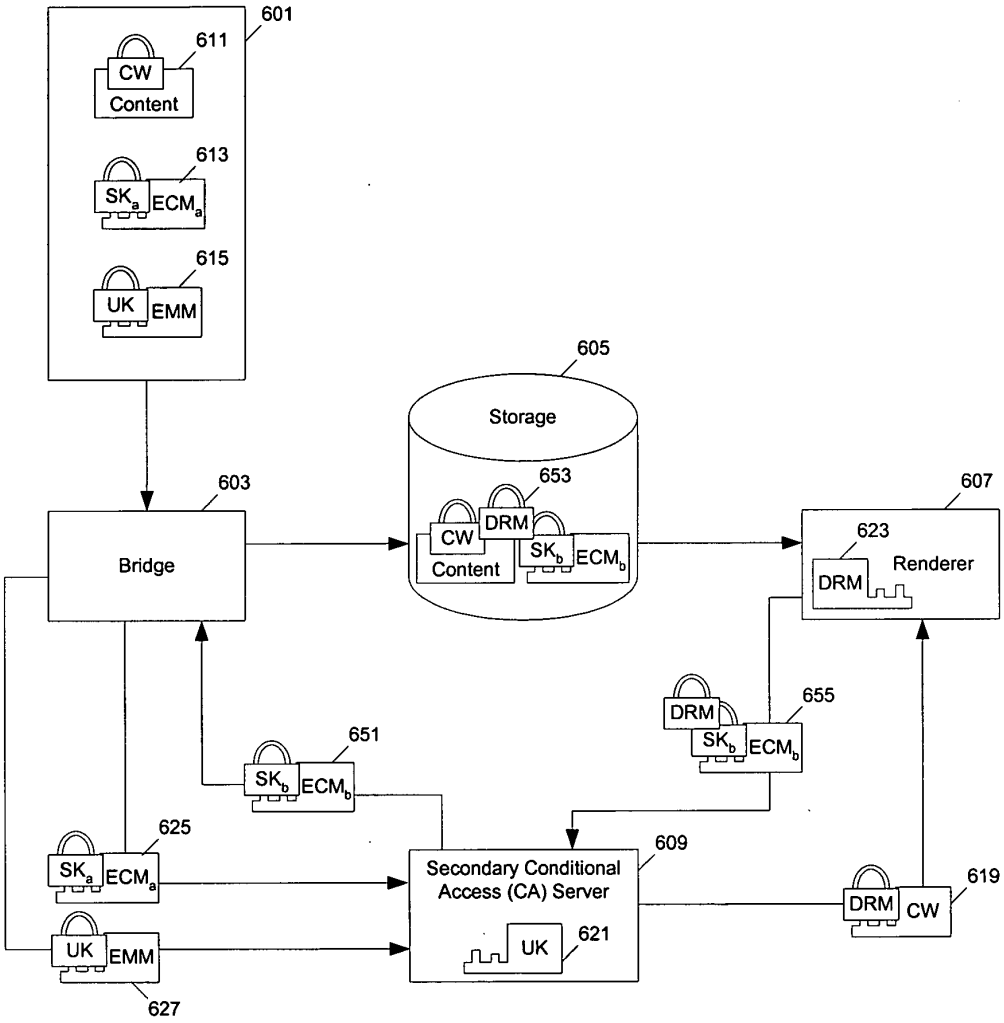

601
611
CW
Content
613
SK_a ECM_a
615
UK EMM
605
Storage
653
DRM
CW
Content
SK_b ECM_b
603
Bridge
607
623
DRM
Renderer
655
DRM
SK_b ECM_b
651
SK_b ECM_b
625
SK_a ECM_a
609
Secondary Conditional Access (CA) Server
UK
621
619
DRM CW
UK EMM
627

Fig. 14

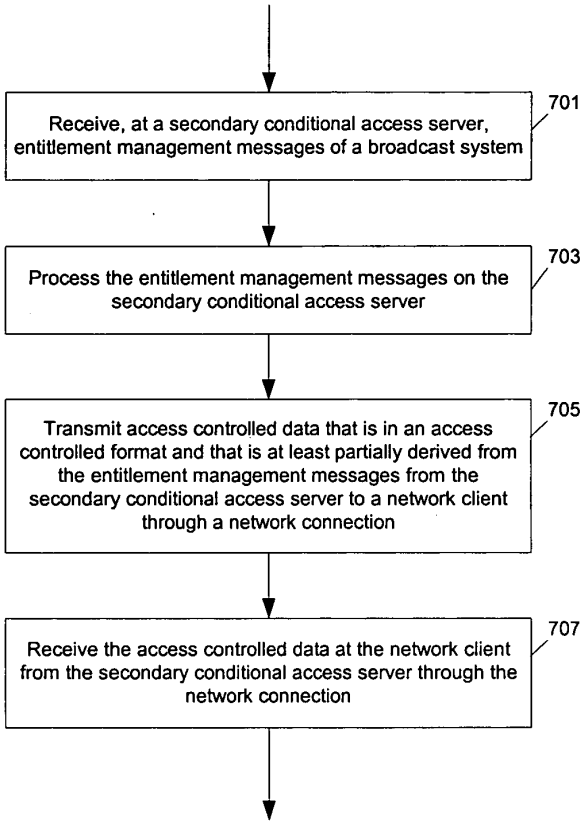

Receive, at a secondary conditional access server, entitlement management messages of a broadcast system
701
Process the entitlement management messages on the secondary conditional access server
703
Transmit access controlled data that is in an access controlled format and that is at least partially derived from the entitlement management messages from the secondary conditional access server to a network client through a network connection
705
Receive the access controlled data at the network client from the secondary conditional access server through the network connection
707

Fig. 15

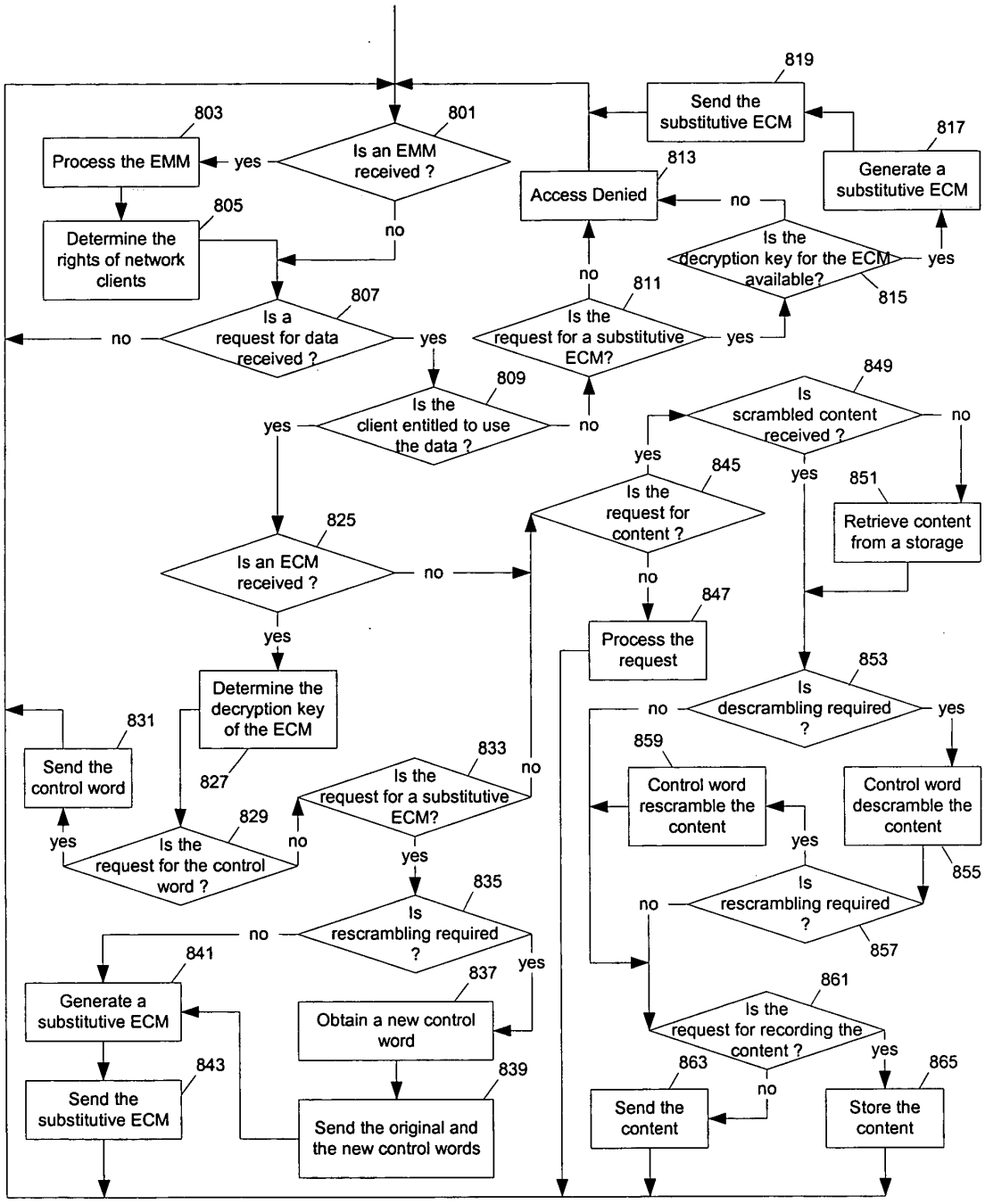

819
Send the substitutive ECM
803
Process the EMM
801
Is an EMM received ?
yes
817
Generate a substitutive ECM
813
Access Denied
no
805
Determine the rights of network clients
no
Is the decryption key for the ECM available?
yes
815
no
811
807
Is a request for data received ?
no
yes
Is the request for a substitutive ECM?
yes
809
Is the client entitled to use the data ?
yes
no
849
Is scrambled content received ?
no
yes
yes
845
Is the request for content ?
851
Retrieve content from a storage
825
Is an ECM received ?
no
no
847
Process the request
yes
853
Is descrambling required ?
no
yes
Determine the decryption key of the ECM
831
Send the control word
827
833
Is the request for a substitutive ECM?
no
859
Control word rescramble the content
Control word descramble the content
yes
829
Is the request for the control word ?
yes
no
yes
855
Is rescrambling required ?
no
857
835
Is rescrambling required ?
no
yes
841
Generate a substitutive ECM
837
Obtain a new control word
861
Is the request for recording the content ?
yes
843
Send the substitutive ECM
839
Send the original and the new control words
863
Send the content
no
865
Store the content

Fig. 16

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION (37 CFR 1.63)		
☒ Declaration Submitted with Initial Filing	OR	☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16(e)) required)

Attorney Docket Number	6517P002
First Named Inventor	Luc Vantalon
COMPLETE IF KNOWN	
Application Number	
Filing Date	
Art Unit	
Examiner Name	

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below, next to my name.

I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Methods And Apparatuses For Secondary Conditional Access Server

(Title of the Invention)

the specification of which

☒ is attached hereto.

OR

☐ was filed on (if applicable):

or _____ as United States Application Number _____

_____ as PCT International Application Number _____

and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment specifically referred to above.

I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application. I do not know and do not believe that the claimed invention was in public use or on sale in the United States of America more than one year prior to this application, nor do I know or believe that the invention has been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

BEST AVAILABLE COPY

IPR2025-00305
ASUS EX1002 Page 125

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, or inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s):

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?
			☐	☐ Yes ☐ No
			☐	☐ Yes ☐ No
			☐	☐ Yes ☐ No
			☐	☐ Yes ☐ No
			☐	☐ Yes ☐ No

Appointment of Practitioners:

I hereby appoint the practitioners associated with Customer Number: **08791** as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected herewith.

If this patent application is assigned, then the undersigned hereby authorizes the patent attorneys and patent agents named herein to accept and follow instructions from the assignee(s) as to any action to be taken in the United States Patent and Trademark Office regarding this application without direct communication between the patent attorneys and patent agents and the undersigned. In the event of a change in the persons from whom instructions may be taken, at least one patent attorney or patent agent named herein will be so notified by the undersigned.

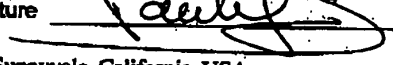
Correspondence:

Direct all correspondence to Customer Number **08791**.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: Luc Vantalon
(First Middle [if any], Family Name (or Surname), and Suffix [if any])

Inventor's Signature  Date 12-06-04

Residence Sunnyvale, California USA *(City, State, Country)* Citizenship France *(Country)*

Mailing Address 868 Helena Drive
Sunnyvale, California 94087 USA

Docket No. 6517P002

BEST AVAILABLE COPY

IPR2025-00305
ASUS EX1002 Page 126

NAME OF SECOND INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: Paolo Siccardo
(First, Middle [if any], Family Name (or Surname), and Suffix [if any])

Inventor's Signature _____ Date Dec 6, 2004

Residence Los Altos, California USA Citizenship USA
(City, State, Country) *(Country)*

Mailing Address 22261 Ainsworth Drive
Los Altos, California 94024 USA

NAME OF THIRD INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: _____
(First, Middle [if any], Family Name (or Surname), and Suffix [if any])

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State, Country) *(Country)*

Mailing Address _____

NAME OF FOURTH INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: _____
(First, Middle [if any], Family Name (or Surname), and Suffix [if any])

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State, Country) *(Country)*

Mailing Address _____

NAME OF FIFTH INVENTOR: ☐ A petition has been filed for this undersigned inventor

Full Name: _____
(First, Middle [if any], Family Name (or Surname), and Suffix [if any])

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State, Country) *(Country)*

Mailing Address _____

BEST AVAILABLE COPY

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

12/10/2004 BSAYASI1 00000008 11007116

01 FC:1001	790.00	OP
02 FC:1201	1056.00	OP
03 FC:1202	2268.00	OP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 489-267/69033

IPR2025-00305
ASUS EX1002 Page 128

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2004

Application or Docket Number: 11e07/16

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	146	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	146 minus 20=	* 126
INDEPENDENT CLAIMS	15 minus 3 =	* 12
MULTIPLE DEPENDENT CLAIM PRESENT		☐

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE	395.00	OR	BASIC FEE	790.00
X$ 9=		OR	X$18=	2268
X44=		OR	X88=	1056
+150=		OR	+300=	1 —
TOTAL		OR	TOTAL	4114

CLAIMS AS AMENDED - PART II

AMENDMENT A		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
	Total	*	Minus	**	=
	Independent	*	Minus	***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐				

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X44=		OR	X88=	
+150=		OR	+300=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
	Total	*	Minus	**	=
	Independent	*	Minus	***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐				

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X44=		OR	X88=	
+150=		OR	+300=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
	Total	*	Minus	**	=
	Independent	*	Minus	***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐				

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X44=		OR	X88=	
+150=		OR	+300=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
***If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

1-10-19-23-28-32-48-62-66-82-96-100-116-130-140-

IPR2025-00305
ASUS EX1002 Page 129

OIPE
FEB 14 2005
JC37
PATENT & TRADEMARK OFFICE

FIW

Attorney Docket No. 06517.P002

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Luc Vantalon, et al

Application No.: 11/007,116

Filing Date: December 7, 2004

For: Methods and Apparatuses for Secondary Conditional Access Server

Examiner: Unknown
Art Unit: 2131

FIRST CLASS CERTIFICATE OF MAILING (37 C.F.R. § 1.8(a))
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

2-9-05
(Date of Deposit)

Joyce Klein
(Name of Person Mailing Correspondence)

(Signature) 2-9-05 (Date)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Examiner:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 together with copies of the documents cited on that form, except for copies not required to be submitted (e.g., copies of U.S. patents and U.S. published patent applications need not be enclosed). It is respectfully requested that the cited documents be considered and that the enclosed copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not

IPR2025-00305
ASUS EX1002 Page 130

to be construed as an admission that the information cited in this statement is material to patentability.

Pursuant to 37 C.F.R. § 1.97, this Information Disclosure Statement is being submitted under one of the following (as indicated by an "X" to the left of the appropriate paragraph):

__x__ 37 C.F.R. §1.97(b).

_____ 37 C.F.R. §1.97(c). If so, then enclosed with this Information Disclosure Statement is one of the following:

____ A statement pursuant to 37 C.F.R. §1.97(e); or

____ A check for $180.00 for the fee under 37 C.F.R. § 1.17(p).

_____ 37 C.F.R. §1.97(d). If so, then enclosed with this Information Disclosure Statement are the following:

(1) A statement pursuant to 37 C.F.R. §1.97(e); and

(2) A check for $180.00 for the fee under 37 C.F.R. §1.17(p) for submission of the Information Disclosure Statement.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

Dated: 2/9, 2005

Lehua Wang
Reg. No. 48,023

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025-1026
(408) 720-8300

Substitute for Form 1449A/PTO (Modified) (use as many sheets as necessary)	Attorney Docket No.: 6517.P002	Application Number: 11/007,116
	First Named Inventor: Luc Vantalon	
	Filing Date: 12/7/2004	

OIPE
FEB 14 2005
PATENT & TRADEMARK OFFICE
TC37

OTHER ART – NO PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	Translation[2]
		InterTrust's Right/System Platform. InterTrust Technologies Corp.	
		Conditional Access (CA) Tutorial. Digital TV Group. www.dtg.org.uk/reference/tutorial/ca.htm. August 2004. 2 pages.	
		RENATO IANNELLA. "Digital Rights Management (DRM) Architectures". D-Lib Magazine, June 2001. Volume 7, Number 6. ISSN 1082-9873. Pages 1-10.	
		MARK MASSEL. "Conditional Access". Broadcasting Engineering, October 2001.	
		ATSC Standard: Conditional Access System for Terrestrial Broadcast, Revision A. Advanced Television Systems Committee, July 2004. Pages 1-31.	

Examiner Signature		Date Considered	

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication.

[1]Unique citation designation number. [2]Applicant is to place a check mark here if English language Translation is attached.

OIPE JC37
FEB 14 2005
PATENT & TRADEMARK OFFICE

TRANSMITTAL **PATENT**

Application No.: 10/007,116
Filing Date: December 7, 2004
First Named Inventor: Luc Vantalon
Examiner's Name: Unknown
Art Unit: 2131
Attorney Docket No.: 06517.P002

____ An Amendment After Final Action (37 CFR 1.116) is attached and applicant(s) request expedited action.
__X__ Charge any fee not covered by any check submitted to Deposit Account No. 02-2666.
__X__ Applicant(s) hereby request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 CFR 1.16 and 1.17, for any concurrent or future reply to Deposit Account No. 02-2666.
____ Applicant(s) claim small entity status (37 CFR 1.27).

ATTACHMENTS

____ Preliminary Amendment
____ Amendment/Response with respect to Office Action
____ Amendment/Response After Final Action (37 CFR 1.116) (reminder: consider filing a Notice of Appeal)
____ Notice of Appeal
____ RCE (Request for Continued Examination)
____ Supplemental Declaration
____ Terminal Disclaimer (reminder: if executed by an attorney, the attorney must be properly of record)
__X__ Information Disclosure Statement (IDS)
__X__ Copies of IDS citations
____ Petition for Extension of Time
____ Fee Transmittal Document (that includes a fee calculation based on the type and number of claims)
____ Cross-Reference to Related Application(s)
____ Certified Copy of Priority Document
____ Other: _____
____ Other: _____
____ Check(s)
__X__ Postcard (Return Receipt)

SUBMITTED BY:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
TYPED OR PRINTED NAME: Lehua Wang
SIGNATURE:. Lehua Wang
REG. NO.: 48,023
DATE: 2/9/2005
ADDRESS: 12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025
TELEPHONE NO.: (408) 720-8300

CERTIFICATE OF MAILING BY FIRST CLASS MAIL (if applicable)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria Virginia 22313-1450 on

2-9-05
Date of Deposit

Joyce Klein
Name of Person Mailing Correspondence

Signature

2-9-05
Date

(10/14/03)

Send to: COMMISSIONER FOR PATENTS, P.O. Box 1450, Alexandria, Virginia 22313-1450

IPR2025-00305
ASUS EX1002 Page 133

CLAIMS ONLY	Application Number 11007116	Filing Date
	Applicant(s)	

* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT		*			*		*	
	Indep	Depend	Indep	Depend	Indep	Depend		Indep	Depend	Indep	Depend	Indep	Depend
1	1						51						
2							52						
3							53						
4							54						
5							55						
6							56						
7							57						
8							58						
9							59						
10	1						60						
11							61						
12							62	1					
13							63						
14							64						
15							65						
16							66	1					
17							67						
18							68						
19	1						69						
20							70						
21							71						
22							72						
23	1						73						
24							74						
25							75						
26							76						
27							77						
28	1						78						
29							79						
30							80						
31							81						
32	1						82	1					
33							83						
34							84						
35							85						
36							86						
37							87						
38							88						
39							89						
40							90						
41							91						
42							92						
43							93						
44							94						
45							95						
46							96	1					
47							97						
48	1						98						
49							99						
50							100	1					
Total Indep							Total Indep						
Total Depend							Total Depend						
Total Claims							Total Claims						

IPR2025-00305
ASUS EX1002 Page 134

CLAIMS ONLY	Application Number 11007116	Filing Date
	Applicant(s)	

* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT		*					
	Indep	Depend	Indep	Depend	Indep	Depend	Indep	Depend	Indep	Depend	Indep	Depend
1		1					51					
2		1					52					
3		1					53					
4		1					54					
5		1					55					
6		1					56					
7		1					57					
8		1					58					
9		1					59					
10		1					60					
11		1					61					
12		1					62					
13		1					63					
14		1					64					
15		1					65					
16	1						66					
17		1					67					
18		1					68					
19		1					69					
20		1					70					
21		1					71					
22		1					72					
23		1					73					
24		1					74					
25		1					75					
26		1					76					
27		1					77					
28		1					78					
29		1					79					
30	1						80					
31		1					81					
32		1					82					
33		1					83					
34		1					84					
35		1					85					
36		1					86					
37		1					87					
38		1					88					
39		1					89					
40	1						90					
41		1					91					
42		1					92					
43		1					93					
44		1					94					
45		1					95					
46		1					96					
47							97					
48							98					
49							99					
50							100					
Total Indep							Total Indep	15				
Total Depend							Total Depend	131				
Total Claims							Total Claims	146				

IPR2025-00305
ASUS EX1002 Page 135

11-07-05 IFW

BLAKELY SOKOLOFF TAYLOR & ZAFMAN

A LIMITED LIABILITY PARTNERSHIP INCLUDING LAW CORPORATIONS

TELEPHONE (408) 720-8300
FACSIMILE (408) 720-8383
BSTZ_MAIL@BSTZ.COM
WWW.BSTZ.COM



INTELLECTUAL PROPERTY LAW

SILICON VALLEY

1279 OAKMEAD PARKWAY
SUNNYVALE, CALIFORNIA 94085-4040

OTHER OFFICES

LOS ANGELES, CA
ORANGE COUNTY/COSTA MESA, CA
SAN JOSE, CA
DENVER, CO
PORTLAND/BEAVERTON, OR
SEATTLE, WA

04 November 2005

MS PG Pub
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Via Express Mail
EV 469 980 229 US

Re: USSN: 11/007,116 Filed: 07 December 2004
Applicant: Digital Keystone, Inc.
Title: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
Transmittal of Request to Rescind Previous Nonpublication Request Under 35 USC 122(b)(2)(B)(ii) and Notification of Foreign Filing Under 35 USC 122(b)(2)(B)(iii)
Our File No.: 6517.P002

Dear Sirs:

We have filed the above-identified application under the Patent Cooperation Treaty. A Request and Certification under 35 USC 122(b)(2)(B)(i) has been submitted for this invention. We herewith submit a Request to Rescind Previous Nonpublication Request under 35 USC 122(b)(2)(B)(ii) and a Notification of Foreign Filing under 35 USC 122(b)(2)(B)(iii).

Respectfully submitted,

Blakely, Sokoloff, Taylor & Zafman LLP

James C. Scheller
Reg. No. 31,195

JCS/SKW/taj
Enclosure

IPR2025-00305
ASUS EX1002 Page 136

OIPE IAP25
NOV 04 2005
PATENT & TRADEMARK OFFICE

RESCISSION OF PREVIOUS NONPUBLICATION REQUEST
(35 U.S.C. 122(b)(2)(B)(ii))
AND, IF APPLICABLE,
NOTICE OF FOREIGN FILING
(35 U.S.C. 122(b)(2)(B)(iii))

Send completed form to:
Mail Stop PG Pub
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
FAX: (703) 305-8568

Application Number 11/007,116
Filing Date 07 December 2004
First Named Inventor Luc Vantalon
Title Methods and Apparatuses for Secondary Conditional Access Server
Attorney Docket No. 6517.P002
Group Art Unit 2131
Examiner Not Yet Assigned

A request that the above-identified application not be published under 35 U.S.C. 122(b) (nonpublication request) was included with the above-identified application on filing pursuant to 35 U.S.C. 122(b)(2)(B)(i). I hereby **rescind** the previous nonpublication request.

If a notice of foreign or international filing is or will be required by 35 U.S.C. 122(b)(2)(B) (iii) and 37 CFR 1.213(c), I hereby provide such notice. This notice is being provided no later than forty-five (**45**) days after the date of such foreign or international filing.

If a notice of subsequent foreign or international filing required by 35 U.S.C. 122(b)(2)(B)(iii) and 37 CFR 1.213(c) was not filed within forty-five (45) days after the date of filing of the foreign or international application, the application is ABANDONED, and a petition to revive under 37 CFR 1.137(b) is required. See 37 CFR 1.137(f).

04 November 2005
Date

Signature

(408) 720-8300
Telephone

James C. Scheller
Typed or Printed Name

31,195
Registration No.

This request must be signed in compliance with 37 CFR 1.33(b).

If information or assistance is needed in completing this form, please contact the Pre-Grant Publication Division at (703) 605-4283 or by e-mail at PGPub@USPTO.gov.

EXPRESS MAIL STATEMENT

"Express Mail" mailing label number: EV 469 980 229 US

Date of Deposit: 04 November 2005

I hereby state that I am causing this correspondence to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this correspondence has been addressed to: Mail Stop PG Pub, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Name (Print/Type) Theresa Joenks

Signature Theresa Joenks Date Signed 11/4/05

Based on Form PTO/SB/36 (05-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 05/09/03

IPR2025-00305
ASUS EX1002 Page 137

FILE COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002

CONFIRMATION NO. 9254

08791
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

Date Mailed: 11/14/2005

Communication Regarding Rescission Of Nonpublication Request and/or Notice of Foreign Filing

Applicant's rescission of the previously-filed nonpublication request and/or notice of foreign filing is acknowledged. The paper has been reflected in the Patent and Trademark Office's (USPTO's) computer records so that the earliest possible projected publication date can be assigned.

The projected publication date is 06/08/2006.

If applicant rescinded the nonpublication request before or on the date of "foreign filing,"[1] then no notice of foreign filing is required.

If applicant foreign filed the application after filing the above application and before filing the rescission, and the rescission did not also include a notice of foreign filing, then a notice of foreign filing (not merely a rescission) is required to be filed within 45 days of the date of foreign filing. See 35 U.S.C. § 122(b)(2)(B)(iii), and Clarification of the United States Patent and Trademark Office's Interpretation of the Provisions of 35 U.S.C. § 122(b)(2)(B)(ii)-(iv), 1272 Off. Gaz. Pat. Office 22 (July 1, 2003).

If a notice of foreign filing is required and is not filed within 45 days of the date of foreign filing, then the application becomes abandoned pursuant to 35 U.S.C. § 122(b)(2)(B)(iii). In this situation, applicant should either file a petition to revive or notify the Office that the application is abandoned. See 37 CFR 1.137(f). Any such petition to revive will be forwarded to the Office of Petitions for a decision. Note that the filing of the petition will not operate to stay any period of reply that may be running against the application.

Questions regarding petitions to revive should be directed to the Office of Petitions at (571) 272-3282. Questions regarding publications of patent applications should be directed to the patent application publication hotline at (703) 605-4283 or by e-mail pgpub@uspto.gov.

[1] Note, for purpose of this notice, that "foreign filing" means "filing an application directed to the same invention in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing".

IPR2025-00305
ASUS EX1002 Page 138

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 843 257**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **02 09878**

(51) Int Cl[7] : **H 04 L 9/14**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 02.08.02.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 06.02.04 Bulletin 04/06.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *VIACCESS Société anonyme* — FR.

(72) **Inventeur(s) :** DUBROEUCQ GILLES et VIGARIE JEAN PIERRE.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** BREVALEX.

(54) PROCEDE ET SYSTEME D'ACCES CONDITIONNEL APPLIQUE A LA PROTECTION DE CONTENU.

(57) L'invention concerne un procédé de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé.

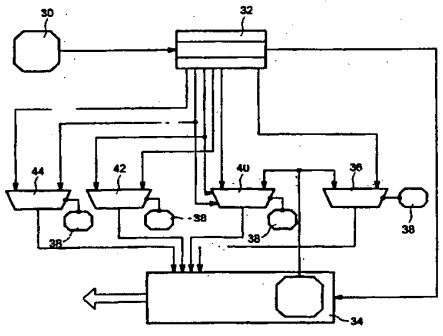
Le procédé selon l'invention comporte les étapes suivantes:

à l'émission:

- générer un message R-ECM$_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux en fonction d'une clé KR$_c$ et d'au moins un critère CRR définissant un droit à l'enregistrement,
- générer un message P-ECM$_c$ de contrôle de titre d'accès à la relecture du contenu du flux enregistré en fonction d'une clé KP$_c$ et d'au moins un critère CRP définissant un droit à la relecture, et

à la réception:

- analyser les messages R-ECM$_c$ et P-ECM$_c$,
- autoriser l'enregistrement et la relecture si les critères CRR et CRP sont vérifiés,



FR 2 843 257 - A1

PROCEDE ET SYSTEME D'ACCES CONDITIONNEL APPLIQUE A LA PROTECTION DE CONTENU

DESCRIPTION

DOMAINE TECHNIQUE

L'invention se situe dans le domaine du contrôle d'accès et concerne plus particulièrement un procédé et un système d'émission/réception d'informations avec contrôle d'accès à travers un réseau de diffusion MPEG2. Ce procédé est applicable à tout flux de données multiplexé reposant sur l'usage de paquet ou trame.

L'invention concerne également une plate-forme d'embrouillage et un récepteur de désembrouillage destinés à mettre en œuvre ce procédé.

Plus spécifiquement, l'invention concerne un procédé et un système de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé par une clé de chiffrement CW transmise sous forme chiffrée dans un message de contrôle de titre d'accès ECM (pour "Entitlement Control Message") comportant au moins un critère CA de contrôle d'accès aux données du flux. Les données transmises étant susceptibles d'être déchiffrées à la volée ou enregistrées telles quelles dans un terminal récepteur.

ETAT DE LA TECHNIQUE ANTERIEURE

Afin de lutter contre le piratage de données et de services distribués en ligne, notamment via le réseau Internet, il devient primordial pour les

opérateurs de protéger ces données en phase de diffusion et après la diffusion.

La figure 1 représente un schéma général d'un système de contrôle d'accès de l'art antérieur dans lequel une plate-forme d'embrouillage 2, agencée généralement en tête de réseau, reçoit un flux en clair F_x et fournit à un terminal récepteur 4 un contenu chiffré F_{xs}. La plate-forme 2 comporte un générateur 6 de clés CWi d'embrouillage et de désembrouillage , un générateur messages de contrôle de titre d'accès (ECM) 8, et un générateur messages de gestion de titre d'accès (EMM) (pour "Entitlement Management Message) 10. Le terminal récepteur 4 comporte un module de désembrouillage 12, un processeur de sécurité 14 comportant un module de déchiffrage 16 des clés de contrôle CW_i et une mémoire 18.

Avant la diffusion des flux de données, ceux-ci sont embrouillés par la plate-forme d'embrouillage 2 au moyen des clés CWi. Afin de permettre le désembrouillage du contenu des flux diffusés, les clés de désembrouillage CW_i sont transmises aux terminaux 4 sous forme chiffrée dans les messages de contrôle de titre d'accès ECM avec au moins un critère CA de contrôle d'accès. Après vérification des critères d'accès au moyen d'un comparateur 20 à des droits préalablement transmis aux terminaux 4, dans les messages de gestion de titre d'accès (EMM) et inscrits dans la mémoire 18, les clés de désembrouillage CW_i sont déchiffrées puis transmises au module de désembrouillage 12.

Pour améliorer la sécurité globale du système, les clés de désembrouillage CW_i changent régulièrement sur des crypto-périodes CP_i (typiquement quelques secondes) et sont généralement appliquées au désembrouilleur 12 par couple $[CW_i, CW_{i+1}]$ où CW_i représentant la clé de désembrouillage valable pendant la crypto-période CP_i, et CW_{i+1} représentant la clé de désembrouillage valable pendant la crypto-période CP_{i+1}. Chaque clé de désembrouillage à utiliser est référencée par un bit indiquant la parité de i de sorte qu'à chaque changement d'ECM, deux clés de désembrouillage, une paire ECW et une impaire OCW, sont configurées sur le désembrouilleur avant le changement effectif de crypto-période.

Dans un contexte de télédiffusion, une technique connue pour protéger le contenu une fois diffusé consiste à enregistrer ce contenu avec la signalisation d'accès conditionnel associée.

Un premier inconvénient de cette solution provient du fait qu'elle ne permet pas d'associer des critères d'accès distincts pour les phases :

- de visualisation directe du contenu depuis le flux ;
- d'enregistrement du contenu ; et
- de visualisation du flux depuis le contenu enregistré localement.

Un second inconvénient de cette technique provient du fait que les clés secrètes d'exploitation stockées dans un processeur de sécurité et servant au déchiffrement des ECMs sont régulièrement mises à jour. Dans ce cas, les ECM stockés avec le contenu ne sont

plus valides et ce dernier devient inexploitable même si le client a acquis des droits d'utilisation dépassant cette période.

Un troisième inconvénient est lié aux aspects de synchronisation entre la fourniture et l'exploitation des clés de désembrouillage CW_i lors d'une exploitation d'un contenu enregistré. Dans ce cas, la fonction de lecture arrière ne peut pas être réalisée de manière simple, car la valeur anticipée de la prochaine clé de désembrouillage (représentant la clé de désembrouillage précédente) n'est pas fournie dans l'ECM.

Une autre technique connue dans l'art antérieur pour protéger le contenu est l'utilisation d'une solution dite DRM (pour Digital Right Management).

Ce type de solution repose sur :

- l'usage de certificats pour établir une chaîne de confiance entre les composants du système ;
- un chiffrement ou pré-embrouillage du contenu à l'aide d'un algorithme à clé privé ;
- l'envoi en ligne de cette clé privée associée aux droits d'utilisations pour former une licence chiffrée à l'aide d'un algorithme de chiffrement utilisant une clé publique du client.

Cette solution n'est pas adaptée au contexte de la télédiffusion dans lequel l'usage d'une voie de retour n'est pas systématique. De plus, ce type de solution ne permet pas de conditionner l'accès au contenu moyennant la possession de droits inscrits

indifféremment par voie hertzienne ou en ligne dans un processeur de sécurité.

Le but de l'invention est de pallier les inconvénients de l'art antérieur décrits ci-dessus au moyen d'un procédé et d'un dispositif utilisant un processus d'embrouillage basé sur des changements périodiques de mots de contrôle et assurant une compatibilité ascendante avec les systèmes d'accès conditionnel antérieurs.

EXPOSÉ DE L'INVENTION

L'invention préconise un procédé de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé au moyen d'une clé de chiffrement CW transmise sous forme chiffrée dans un message de contrôle de titre d'accès ECM comportant en outre au moins un critère CA de contrôle d'accès, lesdites données numériques étant susceptibles d'être enregistrées telles quelles dans un terminal récepteur ou déchiffrées à la volée.

Selon l'invention, ce procédé comporte les étapes suivantes :

à l'émission :

- générer un message $R\text{-}ECM_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux en fonction d'une clé d'enregistrement KR_c et d'au moins un critère CRR définissant un droit à l'enregistrement,
- générer un message $P\text{-}ECM_c$ de contrôle de titre d'accès à la relecture du contenu du flux enregistré en fonction d'une clé de relecture KP_c et d'au moins

IPR2025-00305
ASUS EX1002 Page 144

un critère CRP définissant un droit à la relecture, et

à la réception :

- analyser le message R-ECM_c, et
- autoriser l'enregistrement si le critère CRR est vérifié, sinon, interdire l'enregistrement,
- analyser le message P-ECM_c, et
- autoriser la relecture si le critère CRP est vérifié, sinon, interdire la relecture.

Selon une première variante de réalisation du procédé de l'invention, les clés CW, KR_c et KP_c sont chiffrées par une première clé de service K_s.

Selon une deuxième variante de réalisation du procédé de l'invention les clés CW, KR_c et KP_c sont chiffrées par trois clés de service différentes respectivement K_S, K_{SR} et K_{SP}.

Dans un premier mode de réalisation, la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i, et à chaque changement de crypto-période,
- embrouiller le contenu du flux au moyen de la clé CW_i, et mémoriser une valeur p(i) représentative de la parité de i,
- calculer un message de contrôle de titre d'accès SC-ECM_i en fonction des clés de chiffrement

CW_{i-1}, CW_i, CW_{i+1} préalablement définies, de la valeur p(i) et du critère CA_i, ledit message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen de la clé de relecture KP_c,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c.

Dans un deuxième mode de réalisation, la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données :

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i, et, à chaque changement de crypto-période i,

- embrouiller le contenu du flux au moyen de la clé CW_i, et mémoriser une valeur p(i) représentative de la parité de i,

- calculer un message de contrôle de titre d'accès $SC\text{-}ECM_i$ en fonction des clés de chiffrement CW_{i-1}, CW_i, CW_{i+1} préalablement définies, de la valeur p(i) et du critère CA_i, ledit message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

IPR2025-00305
ASUS EX1002 Page 146

- chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen d'une deuxième clé de service K'_s,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé de relecture KP_c,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c.

Dans les deux modes de réalisation, la phase de l'émission comporte en outre les étapes consistant :

- calculer le message de contrôle de titre d'accès $ECM_i = f[(ECW_i, OCW_i, CA)]$ où, ECW_i et OCW_i représentent respectivement les mots de contrôle pair et impair préalablement chiffrés au moyen d'une première clé de service K_s,

$ECW_i = CW_i$ si i pair sinon $ECW_i = CW_{i+1}$;

$OCW_i = CW_i$ si i impair sinon $OCW_i = CW_{i+1}$;

- diffuser dans la signalisation ECM des paramètres identifiant les voies ECM rattachées au service diffusant le contenu des messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$,

- fournir au terminal récepteur les messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$

Deux modes de distribution des messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ sont possibles. Ces derniers peuvent être soit diffusés sur la voie ECM associée au contenu du segment S_i, soit délivrés en partie au terminal récepteur à partir d'un Serveur

d'Autorisation en tête de réseau sur requête et en fonction du type d'exploitation du contenu envisagé.

Ainsi, les message R-ECM et/ou P-ECM peuvent être délivrés au terminal récepteur sur requête à partir d'un Serveur d'Autorisation en tête de réseau si l'enregistrement et/ou la relecture sont envisagés.

Selon l'invention, pour recevoir directement le flux reçu, la phase de la réception comporte les étapes suivantes :

- récupérer la voie ECM du message ECM_i à partir de la signalisation rattachée au service diffusant le flux de données, et à chaque changement de i,

- analyser le message ECM_i afin de récupérer les mots de contrôle pair OCW, et impair ECW, pour désembrouiller le contenu du flux diffusé de manière à obtenir un accès direct à ce contenu.

Pour enregistrer le flux reçu, la phase de la réception comporte les étapes suivantes :

- récupérer la voie ECM des messages $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ à partir de la signalisation rattachée au service diffusant le contenu ;

- analyser le message $R\text{-}ECM_c$ pour vérifier les critères d'accès à l'enregistrement CRR

- mémoriser la clé d'enregistrement KR_c ;

- récupérer le message $P\text{-}ECM_c$ et le stocker avec le contenu ; et

pour chaque crypto-période i :

- récupérer le message $SC\text{-}ECM_i$,

- déchiffrer le message $SC\text{-}ECM_i$ au moyen de la clé d'enregistrement KR_c, et

- enregistrer le message $SC\text{-}ECM_I$ déchiffré avec le contenu.

Selon l'invention, l'accès à la relecture du contenu du flux enregistré est obtenu selon les étapes suivantes :

- récupérer le message $P\text{-}ECM_c$ dans le contenu et l'analyser pour vérifier les critères d'accès à la lecture CRP,
- mémoriser la clé de relecture KP_c ; et
- récupérer dans le contenu le message $SC\text{-}ECM_i$ courant ;
- déchiffrer le message $SC\text{-}ECM_i$ avec la clé de relecture KP_c et vérifier les critères d'accès,
- récupérer les clés chiffrées CW_{i-1}, CW_i, CW_{i+1} et la valeur p(i) indiquant la parité de i, et
- déchiffrer, au moyen de la deuxième clé K'_s, lesdites clés suivant le sens de lecture pour en déduire ECW et OCW ; puis,
- appliquer soit ECW, soit OCW pour désembrouiller le contenu à la relecture.

Dans une autre variante, l'accès à la relecture du contenu du flux est obtenu selon les étapes suivantes :

- récupérer le message $P\text{-}ECM_c$ dans le contenu,
- analyser le message $P\text{-}ECM_c$ pour vérifier les critères d'accès à la lecture CRP,
- mémoriser KP_c, et
- récupérer dans le contenu le message $SC\text{-}ECM_i$ courant,

SDOCID: <FR _2843257A1_I_>

IPR2025-00305
ASUS EX1002 Page 149

- déchiffrer le message SC-ECM$_i$ avec la deuxième clé de service K'$_s$ et vérifier les critères d'accès,

- récupérer les clés chiffrés CW$_{i-1}$, CW$_i$, CW$_{i+1}$ et la valeur p(i) indiquant la parité de i, et

- déchiffrer, au moyen de la deuxième clé KRc lesdites clés suivant le sens de lecture pour en déduire ECW et OCW ; puis,

- appliquer soit ECW, soit OCW pour désembrouiller le contenu.

Préférentiellement, la phase de réception comporte en outre les étapes suivantes :

- générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,

- sur-chiffrer localement le contenu à enregistrer par cette clé K_I.

- à la relecture, regénérer la clé K_I à partir d'attributs contenus dans le message P-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,

- déchiffrer le contenu enregistré au moyen de la clé K_I regénérée.

Dans une application particulière du procédé selon l'invention, les données numériques diffusées représentent des programmes audiovisuels.

L'invention concerne également un système de contrôle d'accès à un flux de données numériques comportant une plate-forme d'embrouillage comprenant au moins un générateur de messages de contrôle de titre d'accès ECM et au moins un récepteur de désembrouillage muni d'un processeur de sécurité.

Selon l'invention, la plate-forme d'embrouillage comporte en outre:

- un générateur de messages R-ECM$_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux reçu et un générateur de messages P-ECM$_c$ de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré, et le récepteur de désembrouillage comporte :

- des moyens pour récupérer la voie ECM des messages P-ECM$_c$, R-ECM$_c$,

- des moyens pour déchiffrer le contenu d'un flux reçu pour l'enregistrer,

- des moyens pour déchiffrer le contenu d'un flux enregistré pour le relire.

Préférentiellement, le récepteur de désembrouillage comporte en outre des moyens pour générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM et de l'identité du terminal-récepteur pour chiffrer/déchiffrer localement le contenu du flux reçu.

L'invention concerne également une plate-forme d'embrouillage comportant au moins un générateur de messages de contrôle de titre d'accès ECM à un flux de donnée diffusé sous forme embrouillée, un générateur de messages R-ECM$_c$ de contrôle de titre d'accès à

l'enregistrement du contenu d'un flux reçu et un générateur de messages P-ECM_c de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré.

La plate-forme d'embrouillage comporte en outre :

- des moyens pour découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i,
- des moyens pour chiffrer le contenu du flux à chaque changement de crypto-période i au moyen de la clé CW_i,
- des moyens pour calculer un message de contrôle de titre d'accès SC-ECM_i en fonction des clés CW_{i-1}, CW_i, CW_{i+1} correspondant respectivement aux crypto-périodes CP_i, CP_{i-1} et CP_{i+1}, d'un paramètre de parité p(i) et du critère de contrôle d'accès CA_i, ledit message SC-ECM_i étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,
- des moyens pour chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen d'une clé de relecture KP_c,
- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,
- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une clé d'enregistrement KR_c.

L'invention concerne également un récepteur de désembrouillage d'un flux de donné diffusé sous forme embrouillée par une clé d'embrouillage CW_i

comportant un processeur de sécurité dans lequel est mémorisée au moins une clé d'enregistrement KR_c destinée à désembrouiller des messages de contrôle d'accès à l'enregistrement $R\text{-}ECM_c$ et au moins une clé de relecture KP_c destinée à désembrouiller des messages de contrôle d'accès à la relecture $P\text{-}ECM_c$,

Selon l'invention, ce récepteur comporte :

- des moyens pour récupérer la voie ECM des messages $P\text{-}ECM_c$, et des messages $R\text{-}ECM_c$ à partir de la signalisation rattachée au service diffusant le contenu ;

- des moyens pour déchiffrer le message $R\text{-}ECM_c$ au moyen de la clé d'enregistrement KR_c pour vérifier le droit à enregistrer le contenu d'un flux reçu,

- des moyens pour déchiffrer le message $P\text{-}ECM_c$ au moyen de la clé de relecture KP_c pour vérifier le droit à relire le contenu d'un flux enregistré,

Préférentiellement, le récepteur selon l'invention comporte en outre des moyens pour générer une clé K_I à partir de l'identité du récepteur pour chiffrer et déchiffrer localement le contenu du flux reçu.

Dans un mode de réalisation préféré de l'invention, le processeur de sécurité est une carte à puce.

BRÈVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va

suivre, prise à titre d'exemple non limitatif, en référence aux figures annexées dans lesquelles :

- la figure 1, décrite précédemment, représente un schéma général d'un système de contrôle d'accès de l'art antérieur ;
- la figure 2 représente un schéma bloc illustrant la phase d'embrouillage des flux à diffuser par un système de contrôle d'accès selon l'invention,
- la figure 3 illustre schématiquement le processus de contrôle d'accès à l'enregistrement d'un flux de données selon l'invention,
- la figure 4 illustre schématiquement le processus de contrôle d'accès à la relecture du flux de données enregistré selon l'invention.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

La description qui suit sera faite dans le cadre d'une application particulière dans laquelle les flux diffusés représentent des programmes audiovisuels nécessitant un droit d'accès.

Dans cette application, le procédé repose sur une diffusion de contenu à travers une structure de paquets multiplexés dont la forme est indiquée à l'annexe 1.

La signalisation du programme diffusant le contenu comprend une description précise indiquant les voies du multiplex par un identifiant de paquet « Packet Identifier » en anglais utiles à la réception du contenu ainsi que la nature des données transmise dans chaque voie (composante son, vidéo ou autre).

Cette signalisation comprend un descripteur d'accès conditionnel "CA_descriptor" indiquant la présence et la localisation des voies transportant les ECMs. Ce descripteur est associé soit au niveau global du programme, soit au niveau de chaque déclaration d'une voie composante.

Le format de ce descripteur est standard dans le cas d'une diffusion MPEG2 ISO13818-1 représenté à l'annexe 2.

Les données privées "private_data_byte" pour le procédé décrit sont décrites dans l'annexe 3 pour un mode de réalisation.

Elles ont un suffixe XID dans l'entête des ECMs et servent de discriminant pour distinguer les ECM véhiculés éventuellement sur la même voie paquet.

Lorsqu'une partie des voies ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ est absente, les combinaisons possibles sont les suivantes :

- voie ECM_i absente : pas de visualisation immédiate ;
- voie $R\text{-}ECM_c$ absente : enregistrement interdit ou si le terminal récepteur dispose d'une voie de retour opérationnelle, se connecter à un Serveur d'Autorisation en tête de réseau délivrant le message $R\text{-}ECM_c$ nécessaire à l'enregistrement du contenu ;
- voie $P\text{-}ECM_c$ absente : lecture interdite ou si le terminal récepteur dispose d'une voie de retour opérationnelle, se connecter à un Serveur d'Autorisation en tête de réseau délivrant le message $P\text{-}ECM_c$ nécessaire à la lecture du contenu enregistré;

- voie SC-ECM$_i$ absente : alors R-ECM$_i$ et P-ECM$_i$ sont absentes et l'enregistrement n'est pas autorisé.

Selon la nature des données transmises, signalisation ou composante audio ou son, la charge utile « payload » en anglais est chiffrée ou non par la plate-forme d'embrouillage 2 et la valeur du champ "Scrambling Control" prend les valeur suivantes :

- le paquet n'est pas embrouillé,
- le paquet est embrouillé par le mot de contrôle pair ECW,
- le paquet est embrouillé par le mot de contrôle impair OCW.

La figure 2 illustre schématiquement la phase d'embrouillage des flux à diffuser par un système de contrôle d'accès selon l'invention.

L'étape 30 consiste à générer une clé secrète d'enregistrement KR_c de contrôle d'accès à l'enregistrement et une clé secrète de relecture KP_c de contrôle d'accès à la relecture.

L'étape 32 consiste à découper, pour chaque flux de données, la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i. Les paquets ainsi constitués sont ensuite appliqués à un module d'embrouillage et de multiplexage 34 qui reçoit parallèlement un message ECM_i contenant les clés de désembrouillage CW_i, CW_{i+1} de contrôle de titre d'accès au contenu du flux et au moins un critère d'accès CA_i, un message SC-ECM_i contenant les clés de désembrouillage CW_{i-1}, CW_i, CW_{i+1} de contrôle de titre

SDOCID: <FR 2843257A1 I >

IPR2025-00305
ASUS EX1002 Page 156

d'accès aux contenu d'un segment S_i de données correspondant à au moins deux crypto-périodes, un message R-ECM$_c$ contenant la clé d'enregistrement KR_c de contrôle d'accès à l'enregistrement du contenu du segment S_i et au moins un critère CRR définissant un droit à l'enregistrement de ce contenu, et un message P-ECM$_c$ contenant la clé de relecture KP_c de contrôle d'accès à la relecture du contenu du segment S_i enregistré et au moins un critère CRP de contrôle d'accès à la relecture du contenu de ce segment.

Préalablement, à l'étape 36, les clés de désembrouillage CW_i, CW_{i+1} sont chiffrées par une première clé secrète de service K_s extraite d'une carte à puce 38, et à l'étape 40, les clés de désembrouillage CW_{i-1}, CW_i, CW_{i+1} sont chiffrées successivement par la clé d'enregistrement KR_c puis par la clé de relecture KP_c, à l'étape 42, la clé KP_c est chiffrée par une deuxième clé de service K'_s extraite de la carte à puce 38, et à l'étape 44, la clé KR_c est chiffrée par la deuxième clé de service K'_s.

Les messages ECM_i, R-ECM$_i$, P-ECM$_i$ et SC-ECM$_i$ à diffuser sont ensuite appliqués au module d'embrouillage et de multiplexage 34 pour être multiplexés avec le paquet de données et transmis au terminal récepteur.

Notons que l'étape 42 revient à réaliser un sur-chiffrage des mots de contrôle CW_{i-1}, CW_i, CW_{i+1} successivement au moyen de la clé de relecture KP_c, de la deuxième clé de service K'_s, puis de la clé d'enregistrement KR_c.

SDOCID: <FR_____2843257A1_I_>

IPR2025-00305
ASUS EX1002 Page 157

Dans une variante de réalisation ce surchiffrage des mots de contrôle CW_{i-1}, CW_i, CW_{i+1} est réalisé successivement au moyen de la clé K'_s, au moyen de la clé de relecture KP_c, puis au moyen de la clé KR_c.

La figure 3 illustre schématiquement la phase de réception et de désembrouillage d'un contenu diffusé en vue de son enregistrement.

L'étape 50 consiste à rechercher les voies ECM présentes des messages P-ECM_c, R-ECM_c, SC-ECM_i dans la signalisation rattachée au service diffusant le contenu.

L'étape 51 n'est réalisée que si le message R-ECM_c est absent de la diffusion. Une condition supplémentaire est que le terminal récepteur dispose d'un dispositif de commutation bidirectionnelle. L'étape 51 consiste à se connecter à un Serveur d'Autorisation en déclinant l'identifiant du contenu à enregistrer et l'identité du terminal client. Selon des critères connus du Serveur d'Autorisation, ce dernier délivre en ligne le R-ECM_c nécessaire à l'enregistrement du contenu.

A l'étape 52, le message R-ECM_c est présenté au processeur de sécurité qui après vérification des critères d'accès à l'enregistrement mémorise la clé KR_c. L'étape 52 n'est réalisée qu'à condition d'une diffusion du message P-ECM_c.

A l'étape 54, le message P-ECM_c est récupéré puis stocké en l'état dans l'entête du fichier de stockage du contenu.

A l'étape 56, pour chaque crypto-période i, le message $SC\text{-}ECM_i$ est récupéré puis présenté au processeur de sécurité qui le déchiffre avec la clé KR_c pour récupérer un message déchiffré $SC\text{-}ECM_i$ qui est ensuite enregistré avec les paquets du multiplex constituant le contenu.

Dans une variante de réalisation, ces paquets du multiplex sont chiffrés localement (étape 58) avec une clé K_I générée à l'étape 60 à partir d'attributs contenus dans le message $K\text{-}EMC_c$ et d'un paramètre relatif à l'identité du décodeur. A titre d'exemple, ce paramètre peut être le numéro de série du décodeur, l'identifiant unique (UA) de la carte à puce ou encore le numéro de série d'un disque dur équipant le terminal récepteur.

La figure 4 illustre schématiquement la phase de désembrouillage d'un contenu enregistré dans un support d'enregistrement 60 en vue de sa relecture.

L'étape 62 consiste à rechercher le message $P\text{-}ECM_c$ dans l'entête du fichier contenant les données du flux.

L'étape 63 suivante n'est réalisée que si le message $P\text{-}ECM_c$ est absent de l'entête du fichier contenant. Une condition supplémentaire est que le terminal dispose d'un dispositif de communication bidirectionnelle. L'étape 63 consiste à se connecter à un Serveur d'Autorisation en déclinant l'identifiant du contenu à lire et l'identité du terminal client. Selon des critères connus du Serveur d'Autorisation, ce dernier délivre en ligne $P\text{-}ECM_c$ nécessaire à la lecture du contenu.

EX1002 - Page 159

IPR2025-00305
ASUS EX1002 Page 159

A l'étape 64, le message P-ECM$_c$ retrouvé est présenté au processeur de sécurité qui après vérification des critères d'accès à la lecture mémorise la clé de relecture KP$_c$ dans la carte à puce 38.

Si le contenu a été préalablement embrouillé localement conformément à l'étape 58 décrite précédemment, la clé locale d'identité K_I est alors calculée à partir des informations d'identité du terminal récepteur (étape 68), et pour chaque crypto-période i, le multiplex du contenu est déchiffré à la lecture à la volée avec la clé K_I (étape 70).

Dans un mode préféré de réalisation de l'invention, à la relecture, la clé K_I est regénérée à partir d'attributs contenus dans le message P-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur et est utilisée pour déchiffrer le contenu enregistré.

A l'étape 72, le message SC-ECM$_i$ courant est récupéré, puis présenté au processeur de sécurité (étape 74) qui le déchiffre avec la clé KP$_c$ pour vérifier les critères d'accès CRP à la relecture et récupérer les mots de contrôle CW_{i-1}, CW_i, CW_{i+1} et la parité de i. Suivant le sens de lecture souhaité, une des clés de désembrouillage ECW ou OCW est fournie au désembrouilleur pour désembrouiller le segment de données S_i.

Dans le cas où le segment S_i doit être visualisé directement, le procédé selon l'invention permet de rechercher la voie ECM et l'indexe des ECM$_i$ dans la signalisation rattachée au service diffusant le contenu à chaque changement de i et d'appliquer l'ECM$_i$

SDOCID: <FR_____2843257A1_I_>

IPR2025-00305
ASUS EX1002 Page 160

au processeur de sécurité pour récupérer les mots de contrôle pair et impair OCW, ECW et les appliquer au désembrouilleur 80.

EX1002 - Page 161

IPR2025-00305
ASUS EX1002 Page 161

ANNEXE 1

Packet IDentifier	Scrambling Control	Payload : Data bytes + padding bytes

Une définition équivalente est

```
CAS_PACKET_UNIT()
{
  Packet IDentifier          x bits ;
  Scrambling_Control         2 bits ;
  Payload  z bytes
}
x+2 multiple de 8 ;
La séquence payload se décompose en Payload()
{
 data bytes                  m octets
 padding bytes               p octets
             }
```

ANNEXE 2

```
CA_descriptor()
{
        descriptor_tag = 0x09          8 bits
        descriptor_length              8 bits
        CA_system_ID                   16 bits
        reserved                                    3 bits
        CA_PID                         13 bits
        for (i=0; i<N; i++) {
                private_data_byte      8 bits
```

ANNEXE 3

```
private data bytes ()
{
  Si Voie ECM présente dans le multiplex (voir) :
{
   ECM_CHANNEL_TAG                          1 octet
indicateur de descripteur voie SC_ECM
   ECM_XID ;                                1 octet
indexe de l'ECM Stream dans la voie paquet
   ECM_CI ;                                 1 octet
version du crypto-algorithme  pour l'ECM Stream
   ECM_SOID ;                               3 octets
référence du jeu de clé privé utilisé pour le Stream
}
  Si Voie SC_ECM présente dans le multiplex :
  (                  // Extension du système
   SC_ECM_CHANNEL_TAG                       1 octet
indicateur de descripteur voie SC_ECM
    PPS_ECM_CI;                             1 octet
Version du crypto-algorithme pour les ECM "contenus"
    SC_ECM_SOID;                            3 octets
SOID des SC_ECM
    SC_ECM_PID ;                            x octets
identité de la voie paquet pour les SC_ECM
    SC_ECM_XID ;                            1 octet
indexe du SC_ECM dans la voie paquet

    Si Voie R_ECM présente dans le multiplex :
    {
     R_ECM_CHANNEL_TAG                      1 octet
indicateur de descripteur voie R_ECM
     R_ECM_SOID;                            3 octets
SOID des R_ECM
     R_ECM_PID ;                            x octets
identité de la voie paquet pour les R_ECM
     R_ECM _ XID;                           1 octet
indexe du R_ECM dans la voie paquet
    }

    Si Voie P_ECM présente dans le multiplex :
    {
     P_ECM_CHANNEL_TAG                      1 octet
indicateur de descripteur voie P_ECM
```

```
        P_ECM_SOID;                          3 octets
    SOID des P_ECM
        P_ECM_PID ;                          x octets
    identité de la voie paquet pour les R_ECM
        P_ECM_ XID;                          1 octet
    indexe du P_ECM dans la voie paquet
        }
      }
```

REVENDICATIONS

1. Procédé de contrôle d'accès à un flux de données numériques diffusé et préalablement embrouillé au moyen d'une clé de chiffrement CW transmise sous forme chiffrée dans un message de contrôle de titre d'accès ECM comportant en outre au moins un critère CA de contrôle d'accès, lesdites données numériques étant susceptibles d'être enregistrées telles quelles dans un terminal récepteur ou déchiffrées à la volée, procédé caractérisé en ce qu'il comporte les étapes suivantes :

à l'émission :

- générer un message $R\text{-}ECM_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux en fonction d'une clé d'enregistrement KR_c et d'au moins un critère CRR définissant un droit à l'enregistrement,
- générer un message $P\text{-}ECM_c$ de contrôle de titre d'accès à la relecture du contenu du flux enregistré en fonction d'une clé de relecture KP_c et d'au moins un critère CRP définissant un droit à la relecture, et

à la réception :

- analyser le message $R\text{-}ECM_c$, et
- autoriser l'enregistrement si le critère CRR est vérifié, sinon, interdire l'enregistrement,
- analyser le message $P\text{-}ECM_c$, et
- autoriser la relecture si le critère CRP est vérifié, sinon, interdire la relecture.

2. Procédé selon la revendication 1, caractérisé en ce que les clés CW, KR_c et KP_c sont chiffrées par une première clé de service K_s.

3. Procédé selon la revendication 1, caractérisé en ce que les clés CW, KR_c et KP_c sont chiffrées par trois clés de service différentes respectivement K_S, K_{SR} et K_{SP}.

4. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i, et à chaque changement de crypto-période,

- embrouiller le contenu du flux au moyen de la clé CW_i, et mémoriser une valeur p(i) représentative de la parité de i,

- calculer un message de contrôle de titre d'accès $SC\text{-}ECM_i$ en fonction des clés de chiffrement CW_{i-1}, CW_i, CW_{i+1} préalablement définies, de la valeur p(i) et du critère CA_i, ledit message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen de la clé de relecture KP_c,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c.

5. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que la phase de l'émission comporte les étapes suivantes :

pour chaque flux de données :

- découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i, et à chaque changement de crypto-période,

- embrouiller le contenu du flux au moyen de la clé CW_i, et mémoriser une valeur p(i) représentative de la parité de i,

- calculer un message de contrôle de titre d'accès $SC\text{-}ECM_i$ en fonction des clés de chiffrement CW_{i-1}, CW_i, CW_{i+1} préalablement définies, de la valeur p(i) et du critère CA_i, ledit message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- chiffrer les clés CW_{i-1}, CW_i, CW_{i+1} au moyen d'une deuxième clé de service K'_s,

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé KP_c,

DOCID: <FR 2843257A1 I >

IPR2025-00305
ASUS EX1002 Page 168

- chiffrer le résultat du chiffrement de l'étape précédente au moyen de la clé d'enregistrement KR_c.

6. Procédé selon les revendications 4 ou 5, caractérisé en ce que la phase de l'émission comporte en outre les étapes consistant :

- calculer le message de contrôle de titre d'accès $ECM_i = f[(ECW_i, OCW_i, CA)]$ où, ECW_i et OCW_i représentent respectivement les mots de contrôle pair et impair préalablement chiffrés au moyen d'une première clé de service K_s,

$ECW_i = CW_i$ si i pair sinon $ECW_i = CW_{i+1}$;

$OCW_i = CW_i$ si i impair sinon $OCW_i = CW_{i+1}$;

- diffuser dans la signalisation ECM des paramètres identifiant les voies ECM rattachées au service diffusant le contenu des messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$,

- fournir au terminal récepteur les messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$.

7. Procédé selon la revendication 6, caractérisé en ce que les messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ sont diffusés par voies ECM associées au contenu du segment S_i.

8. Procédé selon la revendication 6, caractérisé en ce que, le message R-ECM est délivré au terminal récepteur sur requête à partir d'un Serveur d'Autorisation en tête de réseau.

9. Procédé selon la revendication 6, caractérisé en ce que, le message P-ECM est délivré au terminal récepteur sur requête à partir d'un Serveur d'Autorisation en tête de réseau.

10. Procédé selon la revendication 7, caractérisé en ce que la phase de la réception comporte les étapes suivantes :

- récupérer la voie ECM du message ECM_i à partir de la signalisation rattachée au service diffusant le flux de données, et à chaque changement de i,

- analyser le message ECM_i afin de récupérer les mots de contrôle pair OCW, et impair ECW, pour désembrouiller le contenu du flux diffusé de manière à obtenir un accès direct à ce contenu.

11. Procédé selon la revendication 7, caractérisé en ce que la phase de la réception comporte les étapes suivantes :

- récupérer la voie ECM des messages $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ à partir de la signalisation rattachée au service diffusant le contenu ;

- analyser le message $R\text{-}ECM_c$ pour vérifier les critères d'accès à l'enregistrement CRR,

- mémoriser la clé d'enregistrement KR_c ;

- récupérer le message $P\text{-}ECM_c$ et le stocker avec le contenu ; et

pour chaque crypto-période i :

- récupérer le message $SC\text{-}ECM_i$,

- déchiffrer le message SC-ECM_i au moyen de la clé d'enregistrement KR_c, et

- enregistrer le message SC-ECM_I déchiffré avec le contenu.

12. Procédé selon la revendication 7, caractérisé en ce que l'accès à la relecture du contenu du flux enregistré est obtenu selon les étapes suivantes :

- récupérer le message P-ECM_c dans le contenu et l'analyser pour vérifier les critères d'accès à la lecture CRP,

- mémoriser la clé de relecture KP_c ; et

- récupérer dans le contenu le message SC-ECM_i courant,

- déchiffrer le message SC-ECM_i avec la clé de relecture KP_c et vérifier les critères d'accès,

- récupérer les clés chiffrés CW_{i-1}, CW_i, CW_{i+1} et la valeur p(i) indiquant la parité de i, et

- déchiffrer lesdites clés suivant le sens de lecture pour en déduire ECW et OCW, puis,

- appliquer soit ECW, soit OCW pour désembrouiller le contenu à la relecture.

13. Procédé selon la revendication 7, caractérisé en ce que l'accès à la relecture du contenu du flux est obtenu selon les étapes suivantes :

- récupérer le message P-ECM_c dans le contenu,

- analyser le message P-ECM_c pour vérifier les critères d'accès à la lecture CRP,

ISDOCID: <FR 2843257A1 I >

EX1002 - Page 171

IPR2025-00305
ASUS EX1002 Page 171

- mémoriser KP_c, et

- récupérer dans le contenu le message $SC\text{-}ECM_i$ courant ;

- déchiffrer le message $SC\text{-}ECM_i$ avec la deuxième clé de service K'_S et vérifier les critères d'accès,

- récupérer les clés chiffrés CW_{i-1}, CW_i, CW_{i+1} et la valeur p(i) indiquant la parité de i, et

- déchiffrer lesdites clés suivant le sens de lecture pour en déduire ECW et OCW, puis,

- appliquer soit ECW, soit OCW pour désembrouiller le contenu.

14. Procédé selon la revendication 11 ou 12, caractérisé en ce que la phase de réception comporte en outre les étapes suivantes :

- générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,

- sur-chiffrer localement le contenu à enregistrer par cette clé K_I, et

- à la relecture, regénérer la clé K_I à partir d'attributs contenus dans le message P-ECM et d'au moins un paramètre relatif à l'identité du terminal-récepteur,

- déchiffrer le contenu enregistré au moyen de la clé K_I regénérée.

3°OCID <FR 2843257A1 I >

IPR2025-00305
ASUS EX1002 Page 172

15. Procédé selon l'une des revendications 1 à 14, caractérisé en ce que les données numériques diffusées représentent des programmes audiovisuels.

16. Système de contrôle d'accès à un flux de données numériques comportant une plate-forme d'embrouillage (2) comprenant au moins un générateur de messages de contrôle de titre d'accès ECM et au moins un récepteur de désembrouillage (4) muni d'un processeur de sécurité (14), caractérisé en ce que la plate-forme d'embrouillage (2) comporte en outre :

- un générateur de messages $R\text{-}ECM_c$ de contrôle de titre d'accès à l'enregistrement du contenu du flux reçu et un générateur de messages $P\text{-}ECM_c$ de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré, et en ce que le récepteur de désembrouillage (4) comporte :

- des moyens pour récupérer la voie ECM des messages $P\text{-}ECM_c$, $R\text{-}ECM_c$,

- des moyens pour déchiffrer le contenu d'un flux reçu pour l'enregistrer, et

- des moyens pour déchiffrer le contenu d'un flux enregistré pour le relire.

17. Système selon la revendication 16, caractérisé en ce que le récepteur de désembrouillage (4) comporte en outre des moyens pour générer une clé locale K_I à partir d'attributs contenus dans le message $R\text{-}ECM_c$ et de l'identité du terminal-récepteur pour chiffrer/déchiffrer localement le contenu du flux reçu.

18. Plate-forme d'embrouillage (2) comportant au moins un générateur de messages de contrôle de titre d'accès ECM à un flux de donnée diffusé sous forme embrouillée, caractérisée en ce qu'elle comporte en outre un générateur de messages R-ECM$_c$ de contrôle de titre d'accès à l'enregistrement du contenu d'un flux reçu et un générateur de messages P-ECM$_c$ de contrôle de titre d'accès à la relecture du contenu d'un flux enregistré.

19. Plate-forme d'embrouillage selon la revendication 18, caractérisée en ce qu'elle comporte :

- des moyens pour découper la période d'embrouillage en une suite de crypto-périodes Cp$_i$ définissant chacune une durée de validité d'une clé individuelle CW$_i$,

- des moyens pour chiffrer le contenu du flux à chaque changement de crypto-période i au moyen de la clé CW$_i$,

- des moyens pour calculer un message de contrôle de titre d'accès SC-ECM$_i$ en fonction des clés CW$_{i-1}$, CW$_i$, CW$_{i+1}$ correspondant respectivement aux crypto-périodes CP$_i$, CP$_{i-1}$ et CP$_{i+1}$, d'un paramètre de parité p(i) et du critère de contrôle d'accès CA$_i$, ledit message SC-ECM$_i$ étant destiné à véhiculer des droits d'accès à un segment S$_i$ de données correspondant à au moins deux crypto-périodes,

- des moyens pour chiffrer les clés CW$_{i-1}$, CW$_i$, CW$_{i+1}$ au moyen d'une clé de relecture KP$_c$,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une clé d'enregistrement KR_c.

20. plate-forme selon la revendication 18, caractérisé en ce qu'elle comporte en outre :

- des moyens pour découper la période d'embrouillage en une suite de crypto-périodes CP_i définissant chacune une durée de validité d'une clé individuelle CW_i,

- des moyens pour chiffrer le contenu du flux à chaque changement de crypto-période i au moyen de la clé CW_i,

- des moyens pour calculer un message de contrôle de titre d'accès $SC\text{-}ECM_i$ en fonction des clés CW_{i-1}, CW_i, CW_{i+1} correspondant respectivement aux crypto-périodes CP_i, CP_{i-1} et CP_{i+1}, d'un paramètre de parité p(i) et du critère de contrôle d'accès CA_i, le message $SC\text{-}ECM_i$ étant destiné à véhiculer des droits d'accès à un segment S_i de données correspondant à au moins deux crypto-périodes,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une deuxième clé de service K'_s,

- des moyens pour chiffrer les mots de contrôle CW_{i-1}, CW_i, CW_{i+1} au moyen d'une clé de relecture KP_c,

- des moyens pour chiffrer le résultat du chiffrement de l'étape précédente au moyen d'une clé d'enregistrement KR_c.

21. Récepteur de désembrouillage (4) d'un flux de donné diffusé sous forme embrouillée par une clé d'embrouillage CW_i comportant un processeur de sécurité comprenant au moins une clé KR_c destinée à désembrouiller des messages R-ECM_c de contrôle d'accès à l'enregistrement et au moins une clé KP_c destinée à désembrouiller des messages P-ECM_c de contrôle d'accès à la relecture, récepteur caractérisé en ce qu'il comporte :

- des moyens pour récupérer la voie ECM des messages P-ECM_c et des messages R-ECM_c à partir de la signalisation rattachée au service diffusant le contenu ;

- des moyens pour déchiffrer le messages R-ECM_c au moyen de la clé d'enregistrement KR_c pour vérifier le droit à enregistrer le contenu d'un flux reçu,

- des moyens pour déchiffrer le messages P-ECM_c au moyen de la clé KP_c pour vérifier le droit à relire le contenu d'un flux enregistré.

22. Récepteur selon la revendication 21, caractérisé en ce qu'il comporte en outre des moyens pour générer une clé locale K_I à partir d'attributs contenus dans le message R-ECM_c de l'identité du récepteur pour chiffrer et déchiffrer localement le contenu du flux reçu.

23. récepteur selon la revendication 21, caractérisé en ce que le processeur de sécurité est une carte à puce.

SDOCID: <FR_____2843257A1_I_>

IPR2025-00305
ASUS EX1002 Page 177

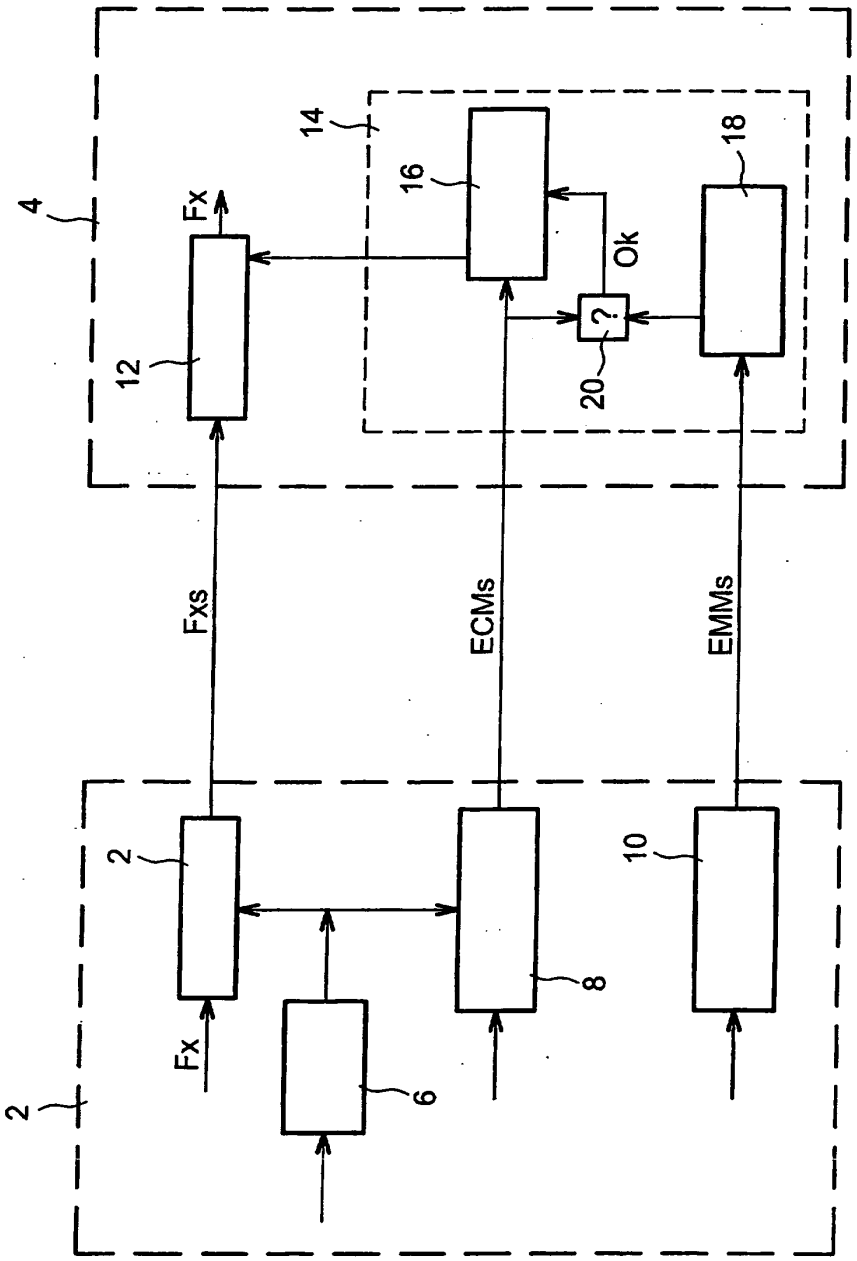


FIG. 1

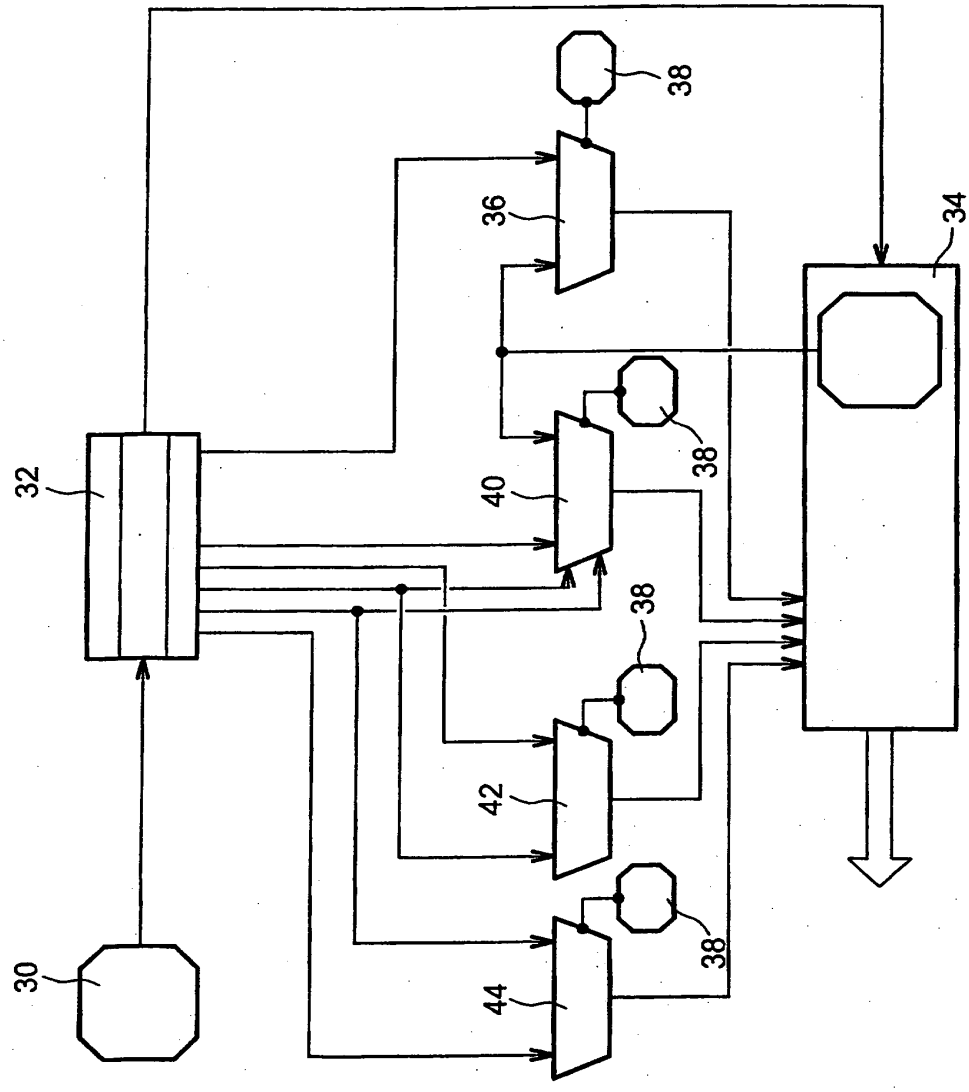


FIG. 2

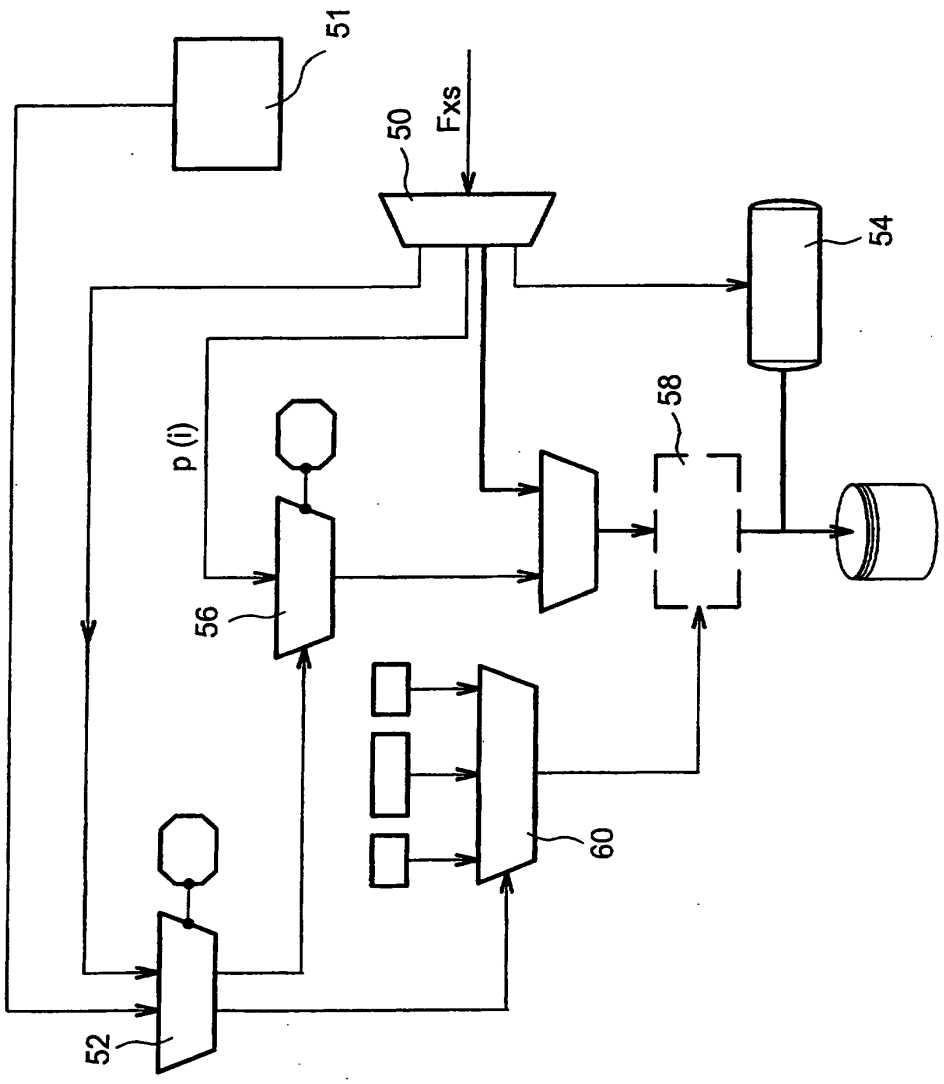


FIG. 3

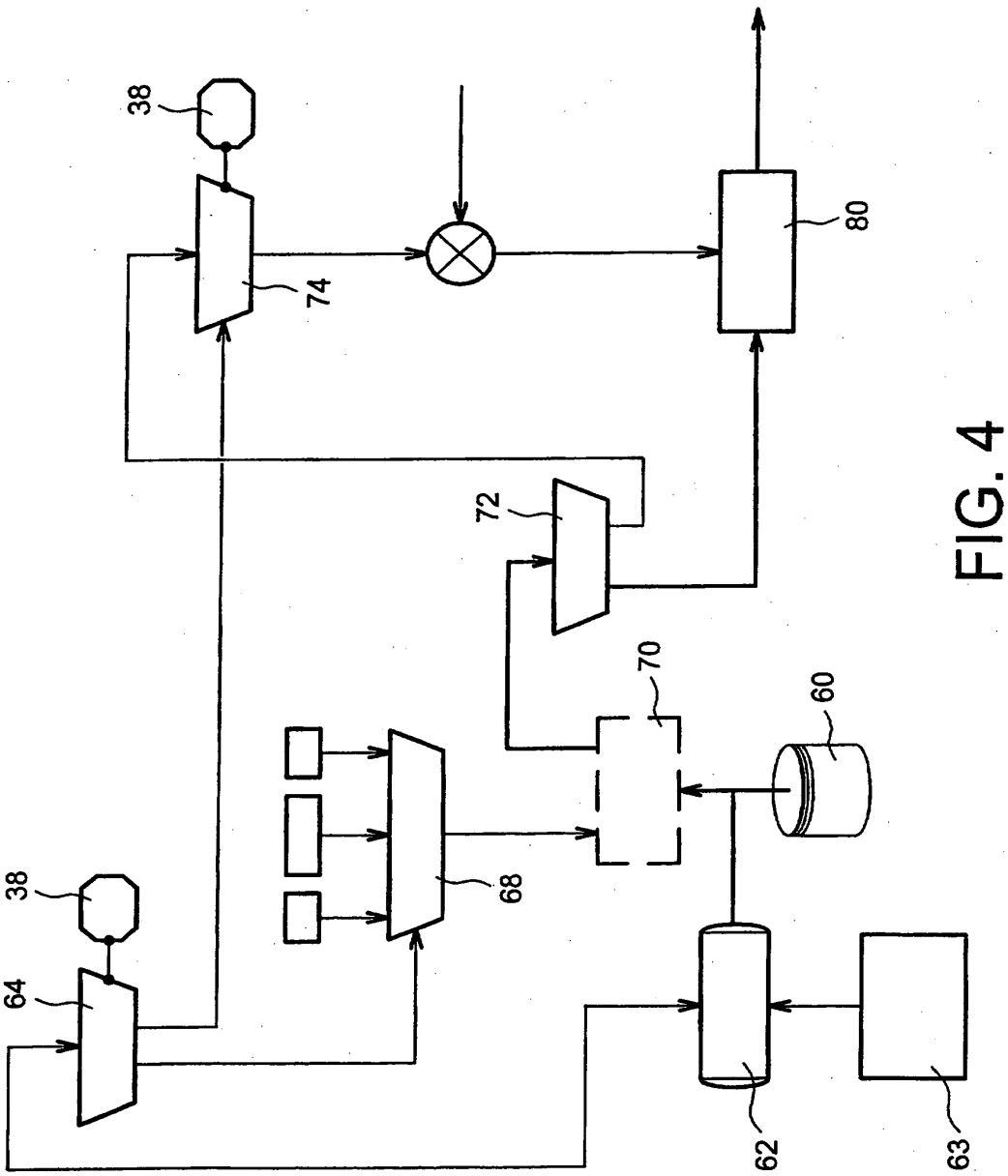


FIG. 4

RÉPUBLIQUE FRANÇAISE

2843257

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 622508
FR 0209878

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	EP 0 936 774 A (CANAL PLUS SA) 18 août 1999 (1999-08-18) * alinéas '0038!,'0039! * * alinéas '0060!,'0062!,'0063! * * alinéas '0068!-'0071! *	1,15,16, 18,21	H04L9/14
Y	EP 0 691 787 A (SONY CORP) 10 janvier 1996 (1996-01-10) * colonne 1, ligne 1 - ligne 24 * * colonne 17, ligne 11 - ligne 34 * * figures 6,7A,7B *	1,15,16, 18,21	
A	EP 0 858 184 A (NDS LTD) 12 août 1998 (1998-08-12) * colonne 3, ligne 2 - ligne 11 * * colonne 3, ligne 32 - ligne 54 *	1-23	
A	US 2001/014974 A1 (YOSHIDA SUNAO ET AL) 16 août 2001 (2001-08-16) * alinéas '0029!,'0030! *	1-23	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.Cl.7)
			H04N H04L

2

Date d'achèvement de la recherche	Examinateur
7 juillet 2003	Tito Martins, J

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0209878 FA 622508

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date d07-07-2003
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0936774 A	18-08-1999	EP 0936774 A1	18-08-1999
		AT 225999 T	15-10-2002
		AU 754015 B2	31-10-2002
		AU 2295199 A	30-08-1999
		AU 749013 B2	13-06-2002
		AU 2296499 A	30-08-1999
		BR 9907877 A	31-10-2000
		BR 9907878 A	31-10-2000
		CA 2318879 A1	19-08-1999
		CA 2318992 A1	19-08-1999
		CN 1305674 T	25-07-2001
		CN 1296695 T	23-05-2001
		DE 69903408 D1	14-11-2002
		DE 69903408 T2	18-06-2003
		EP 0936812 A1	18-08-1999
		EP 1057332 A1	06-12-2000
		EP 1055305 A1	29-11-2000
		ES 2185311 T3	16-04-2003
		HR 20000486 A1	28-02-2001
		HR 20000487 A1	28-02-2001
		HU 0100651 A2	28-06-2001
		HU 0101456 A2	28-09-2001
		WO 9941907 A1	19-08-1999
		WO 9941874 A1	19-08-1999
		JP 2002503919 T	05-02-2002
		JP 2002514834 T	21-05-2002
		NO 20004062 A	13-10-2000
		NO 20004063 A	13-10-2000
		PL 342260 A1	04-06-2001
		PL 342261 A1	04-06-2001
		TR 200002348 T2	21-12-2000
		TR 200002350 T2	22-01-2001
		ZA 9901122 A	30-09-1999
		ZA 9901123 A	12-08-1999
EP 0691787 A	10-01-1996	CN 1390044 A	08-01-2003
		CN 1390043 A	08-01-2003
		CN 1390055 A	08-01-2003
		CN 1390056 A	08-01-2003
		CN 1390057 A	08-01-2003
		CN 1390053 A	08-01-2003
		CN 1389994 A	08-01-2003
		CN 1390054 A	08-01-2003
		CN 1115150 A ,B	17-01-1996
		DE 69523220 D1	22-11-2001
		DE 69523220 T2	13-06-2002

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

SDOCID: <FR 2843257A1_I_>

IPR2025-00305
ASUS EX1002 Page 183

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0209878 FA 622508

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 07-07-2003
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0691787	A		DE	69530622 D1	05-06-2003
			EP	1126705 A2	22-08-2001
			EP	1244306 A2	25-09-2002
			EP	0691787 A1	10-01-1996
			EP	0975165 A2	26-01-2000
			JP	8077706 A	22-03-1996
			JP	2003134104 A	09-05-2003
			JP	2003143547 A	16-05-2003
			JP	2003101942 A	04-04-2003
			JP	2003116120 A	18-04-2003
			JP	2003116101 A	18-04-2003
			JP	2003143548 A	16-05-2003
			US	5796828 A	18-08-1998
			US	RE38007 E1	25-02-2003
EP 0858184	A	12-08-1998	IL	120174 A	28-10-1999
			EP	0858184 A2	12-08-1998
			US	6178242 B1	23-01-2001
			GB	2322030 A ,B	12-08-1998
US 2001014974	A1	16-08-2001	JP	2001223953 A	17-08-2001

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

IPR2025-00305
ASUS EX1002 Page 184

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
6 février 2003 (06.02.2003)

PCT

(10) Numéro de publication internationale
WO 03/010722 A2

(51) Classification internationale des brevets[7] : G07F 7/00

(21) Numéro de la demande internationale :
PCT/EP02/08207

(22) Date de dépôt international : 23 juillet 2002 (23.07.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
101 35 888.1 24 juillet 2001 (24.07.2001) DE

(71) Déposant *(pour tous les États désignés sauf US)* : SCM MICROSYSTEMS GMBH [DE/DE]; Oskar-Messter-Strasse 13, 85737 Ismaning (DE).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : LOISEL, Yann [FR/FR]; Lotissement La Revestin, Chemin des Severiers, F-13600 La Ciotat (FR).

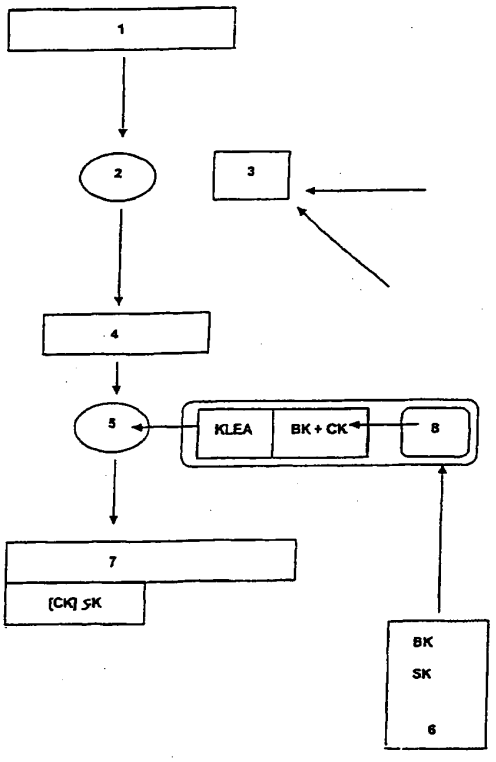
(74) Mandataire : DEGWERT, Hartmut; Prinz & Partner, Manzingerweg 7, 81241 München (DE).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD FOR LOCAL RECORDING OF TELEVISION DIGITAL DATA

(54) Titre : PROCEDE D'ENREGISTREMENT LOCAL DE DONNEES NUMERIQUES POUR LA TELEVISION



(57) Abstract: The invention concerns a method for local recording of digital data received by a transmission network, which consists in encrypting the digital data received with a local recording key (KLEA) and in locally storing the encrypted data (7). The method is characterised in that it comprises the following steps: generating a content key (CK), combining the content key (CK) and a base key (BK) to obtain the local recording key (KLEA), jointly storing the content key (CK) and the encrypted data (7) with the local recording key (KLEA). The invention is particularly applicable to local recording of digital data derived from digital television broadcasting.

(57) Abrégé : La présente invention concerne un procédé d'enregistrement local de données numériques reçues par un réseau de transmission, dans lequel on crypte les données numériques reçues avec une clé locale d'enregistrement (KLEA) et on stocke localement les données cryptées (7). Selon ce procédé, on effectue les étapes suivantes: on génère une clé de contenu (CK), on combine la clé de contenu (CK) et une clé de base (BK) pour obtenir la clé locale d'enregistrement (KLEA), on stocke conjointement la clé de contenu (CK) et les données cryptées (7) avec la clé locale d'enregistrement (KLEA).L'invention s'appliquera tout particulièrement à l'enregistrement local de données issues de diffusion de télévision numérique.

WO 03/010722 A2

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Procédé d'enregistrement local de données numériques pour la télévision numérique

La présente invention concerne un procédé d'enregistrement local de données numériques reçues par un réseau de transmission.

Elle s'applique en particulier au domaine de la télévision numérique pour procéder à un enregistrement local de données reçues par un réseau de transmission numérique, notamment par satellite ou par câbles.

A l'heure actuelle, les programmes de télévision numérique sont reçus par un réseau de transmission au niveau d'un décodeur chez l'utilisateur. Ce décodeur est constitutif d'un dispositif d'accès conditionnel pouvant comprendre différents moyens d'autorisation.

La transmission des données numériques est généralement cryptée pour éviter tout usage illicite par des personnes non autorisées.

Les données sont ensuite décryptées au niveau du dispositif d'accès conditionnel en considérant les autorisations accordées à l'utilisateur. De tels décodeurs permettent généralement afficher directement le flux de données ainsi que décryptées.

Comme le décodeur n'a généralement pas de capacité d'enregistrement, le contenu du programme de télévision numérique est seulement disponible pour être regardé à l'heure de la diffusion. Si l'utilisateur souhaite le regarder à un autre moment, il est alors nécessaire d'effectuer un enregistrement local en respectant les contraintes de re-cryptage pour éviter toute copie illicite au niveau local.

Pour répondre à cet objectif de re-cryptage local, on a déjà pensé à proposer certains dispositifs. Ainsi, les documents US-A-5 897 218 et FR-A- 2 732 537 divulguent un cryptage local pour un enregistrement au niveau du décodeur ou d'un dispositif raccordé à celui-ci. Cependant, les techniques divulguées dans ces

IPR2025-00305
ASUS EX1002 Page 187

documents utilisent le même algorithme de re-cryptage que celui utilisé pour désembrouiller le flux reçu par le réseau de transmission, ce qui en fait une solution propriétaire non généralis.

On connaît également du document EP-A-0 936 812 une méthode d'enregistrement local susceptible d'utiliser un algorithme d'encryption local différent.

En outre, ce document propose l'utilisation de dispositifs portables tels des cartes à puce pour stocker des paramètres importants de cryptage et particulièrement des clés.

Cela étant, la technique présentée selon cette antériorité a l'inconvénient de stocker avec le flux de données cryptées localement l'intégralité de la clé ayant servi à ce cryptage local. Certes cette clé est elle-même brouillée par une autre clé, mais le perçage du cryptage de la clé stockée avec les données permet de recouvrir directement, en clair, l'intégralité du programme de télévision numérique.

Par conséquent, aucune des techniques actuellement connues ne donne entièrement satisfaction quant à l'efficacité du cryptage local effectué.

L'invention permet de remédier aux inconvénients des techniques connues jusqu'alors.

Elle propose pour ce faire un procédé qui permet de combiner au moins deux clés différentes dont l'une d'entre elles seulement est stockée avec les données cryptées localement.

Un personne mal attentionnée ne peut donc, par simple découverte de la clé stockée avec les données cryptées localement, parvenir à leur décryptage.

Un autre objet de l'invention est de faire coopérer un module portable de sécurité, tel une carte à puce, avec un dispositif fixe afin de disposer d'un ensemble plus souple d'utilisation (notamment dans l'attribution des clés, leur

gestion et leur modifications) et plus sûr (en supprimant le stockage et certaines opérations au niveau du décodeur lui-même).

Un autre avantage de l'invention est de permettre la combinaison éventuelle du système d'enregistrement local et du décodeur tel que connu actuellement pour recevoir les données issues du réseau de transmission et les décrypter puis les afficher.

D'autres buts et avantages apparaîtront au cours de la description qui suit qui présente un mode de réalisation préféré de l'invention.

La présente invention concerne un procédé d'enregistrement local de données numériques reçues par un réseau de transmission, dans lequel on crypte les données numériques reçues avec une clé locale d'enregistrement et on stocke localement les données cryptées, caractérisé par le fait

- qu'on génère une clé de contenu,
- qu'on combine la clé de contenu et une clé de base pour obtenir la clé locale d'enregistrement,
- qu'on stocke conjointement la clé de contenu et les données cryptées avec la clé locale d'enregistrement.

Selon des variantes préférées de ce procédé :

- la clé de base est stockée sur un module portable de sécurité,
- on combine la clé de contenu et la clé de base sur le module portable de sécurité,
- on signe la clé de contenu avec une clé de signature avant son stockage conjoint avec les données cryptées,
- on stocke la clé de signature sur un module portable de sécurité,

IPR2025-00305
ASUS EX1002 Page 189

- on génère la clé de contenu de façon aléatoire, à chaque enregistrement d'un flux de données numériques,

- on affiche les données numériques enregistrées par :

- recouvrement de la clé de contenu stockée,
- combinaison de la clé de contenu recouvrée avec la clé de base pour reproduire la clé locale d'enregistrement,
- décryptage des données numériques avec la clé locale d'enregistrement,
- transmission des données numériques aux moyens d'affichage.

- les données numériques sont reçues cryptées du réseau de transmission puis décryptées par un algorithme de cryptage,

- on utilise un algorithme de cryptage différent pour le cryptage avec la clé locale d'enregistrement,

- on utilise des données numériques de diffusion télévisuelle.

Les dessins ci-joints sont donnés à titre d'exemples et ne sont pas limitatifs de l'invention. Ils représentent seulement un mode de réalisation de l'invention et permettront de la comprendre aisément.

La figure 1 est un bloc diagramme des étapes de mise en œuvre de l'invention dans un mode de réalisation préféré,

la figure 2 montre une possibilité de décryptage suite au cryptage local dans un mode de réalisation préféré.

Le procédé selon l'invention pourra être mis en œuvre par un appareil constitué par un boîtier renfermant différents moyens électroniques de cryptage et de décryptage ainsi que des moyens de stockage de données.

EX1002 - Page 190

IPR2025-00305
ASUS EX1002 Page 190

De façon préférée, cet appareil est constitué d'une base comprenant des moyens locaux d'encryptage ainsi que des moyens de mémorisation qui coopèrent avec un ou plusieurs modules portables de sécurité 6 avantageusement constitués par des cartes à puce pouvant répondre à des normes connues.

Cette coopération entre la base de l'appareil et les modules 6 s'effectuera au moyen d'un lecteur adapté.

En se référant à la figure 1, on a d'abord illustré les phases classiques et connues en elles-mêmes de réception et de décryptage d'un flux de données de télévision numériques depuis un réseau, par exemple satellitaire.

A cette figure, des données entrant 1 qui sont cryptées par le fournisseur du programme de télévision numérique parviennent jusqu'à un dispositif d'accès conditionnel 2 présent chez l'utilisateur. Ce dispositif 2 a pour fonction de recevoir, de décrypter et de permettre l'affichage du programme de télévision numérique contenu dans le flux de données reçu.

Pour y parvenir, le dispositif d'accès conditionnel 2 comprend différents moyens de décryptage en fonction d'autorisations accordées à l'utilisateur. De façon préférée, les autorisations accordées à l'utilisateur sont contenues sous forme de clés ou d'autres données dans un module d'accès conditionnel 3, par exemple au format carte à puce. Le module 3 peut être lu par le dispositif 2.

Le flux de données entrant 1 peut être correctement décrypté par le dispositif 2 si l'autorisation est véritable, ce qui permet l'extraction de données en clair 4.

A ce niveau, le programme de télévision numérique peut être directement affiché à l'écran et regardé par le téléspectateur.

Cela étant, il est également possible de réaliser un enregistrement local de ce programme de télévision au moyen du procédé de l'invention.

Dans ce cadre, le repère 5 à la figure 1 représente des moyens locaux d'encryptage permettant de re-crypter localement les données ainsi traitées. Les

IPR2025-00305
ASUS EX1002 Page 191

moyens locaux d'encryptage 5 sont préférentiellement constitués par un algorithme local d'encryptage symétrique distinct de celui utilisé pour le cryptage et le décryptage des données entrant 1 issues du réseau de transmission.

Le cryptage local ainsi effectué par les moyens 5 utilise une clé locale d'enregistrement KLEA. De façon caractéristique à l'invention, cette clé locale d'enregistrement KLEA est une combinaison de plusieurs clés et particulièrement de deux clés différentes de BK et CK.

La clé BK est une clé de base pouvant être stockée sur un module portable de sécurité 6 rapporté à la base de l'appareil d'encryptage local. La clé de base BK peut être réutilisée pour le cryptage de plusieurs programmes de télévision numérique. Le stockage sur un module portable de sécurité tel une carte à puce a l'avantage d'éviter sa communication à la base de l'appareil de cryptage local et d'enregistrement. On peut bien entendu prévoir une mise à jour de la clé de base BK par des transmissions à travers le réseau de transmission pour la diffusion de télévision numérique. On peut également prévoir d'autres mises à jour ainsi que la possibilité d'utilisation de plusieurs clés de base BK selon les fournisseurs de programmes de télévision numérique.

Pour réaliser la clé locale d'enregistrement KLEA, la clé de base BK est combinée avec une autre clé appelée clé de contenu CK. La clé de contenu CK est préférentiellement modifiée à chaque opération de stockage local d'un programme de télévision numérique.

Selon le procédé de l'invention, on génère la clé CK par un générateur 8, et ce préférentiellement de façon aléatoire.

On combine ensuite la clé de contenu CK constitutive d'un nombre aléatoire avec la clé de base BK pour obtenir la clé locale d'enregistrement KLEA servant au cryptage local des données.

Il est ensuite possible de stocker localement dans une mémoire adaptée à la fois le flux de données numériques cryptées par la clé KLEA au moyen des moyens locaux d'encryptage 5 et la clé de contenu CK.

Pour assurer une protection encore plus grande contre le piratage, la clé de contenu CK peut être stockée avec le flux de données numériques ainsi crypté 7 après signature par une clé de signature SK.

Avantageusement, la clé de signature SK est également stockée sur un module portable de sécurité 6.

De façon préférée. l'étape de combinaison de la clé de base BK et de la clé de contenu CK est opérée au sein du module portable de sécurité 6 pour éviter la transmission en clair de la clé de base BK. La génération aléatoire de la clé de contenu CK peut être, elle, effectuée au niveau de la base de l'appareil ou au sein du module portable de sécurité 6. Le générateur 8 de nombres aléatoires sera positionné en fonction.

Comme indiqué en figure 1, le résultat du procédé consiste dans l'enregistrement local de données cryptées 7 conjointement à la clé de contenu CK qui ne constitue qu'une partie de la clé KLEA ayant permis le cryptage.

Bien entendu, d'autres données peuvent être stockées conjointement et notamment les caractéristiques de transmission (date de transmission notamment).

Pour réaliser le décryptage et l'affichage des données cryptées 7, on peut suivre les étapes illustrées en figure 2.

A cette figure, on recouvre la clé de contenu CK directement avec les données cryptées 7, et on vérifie la signature avec la clé de signature SK qui a servi à sa signature.

La clé de contenu CK est ainsi récupérée par le module portable de sécurité 6 et peut subir une recombinaison avec la clé de base BK. Cette nouvelle combinaison assure la reformation de la clé locale d'enregistrement KLEA.

Celle-ci est alors transmise aux moyens locaux d'encryptage 5 pour réaliser un décryptage des données 7.

On récupère alors des données en clair 4 susceptibles d'être affichées.

Revendications

1. Procédé d'enregistrement local de données numériques reçues par un réseau de transmission, dans lequel on crypte les données numériques reçues avec une clé locale d'enregistrement (KLEA) et on stocke localement les données cryptées (7), caractérisé par le fait

- qu'on génère une clé de contenu (CK),

- qu'on combine la clé de contenu (CK) et une clé de base (BK) pour obtenir la clé locale d'enregistrement (KLEA),

- qu'on stocke conjointement la clé de contenu (CK) et les données cryptées (7) avec la clé locale d'enregistrement (KLEA).

2. Procédé selon la revendication 1, caractérisé par le fait que la clé de base (BK) est stockée sur un module portable de sécurité (6).

3. Procédé selon la revendication 2, caractérisé par le fait qu'on combine la clé de contenu (CK) et la clé de base (BK) sur le module portable de sécurité (6).

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé par le fait qu'on signe la clé de contenu (CK) avec une clé de signature (SK) avant son stockage conjoint avec les données cryptées (7).

5. Procédé selon la revendication 4, caractérisé par le fait qu'on stocke la clé de signature (SK) sur un module portable de sécurité (6).

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé par le fait qu'on génère la clé de contenu (CK) de façon aléatoire, à chaque enregistrement d'un flux de données numériques.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé par le fait qu'on affiche les données numériques enregistrées par :

- recouvrement de la clé de contenu (CK) stockée,

- vérification de la signature avec la clé de signature (SK),

- combinaison de la clé de contenu (CK) recouvrée avec la clé de base (BK) pour reproduire la clé locale d'enregistrement (KLEA),

- décryptage des données numériques (7) avec la clé locale d'enregistrement (KLEA)

- transmission des données numériques aux moyens d'affichage.

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé par le fait

- que les données numériques sont reçues cryptées du réseau de transmission puis décryptées par un algorithme de cryptage,

- qu'on utilise un algorithme de cryptage différent pour le cryptage avec la clé locale d'enregistrement (KLEA).

9. Procédé selon l'une quelconque des revendications 1 à 8, caractérisé par le fait qu'on utilise des données numériques de diffusion télévisuelle.

IPR2025-00305
ASUS EX1002 Page 196

FIG. 1

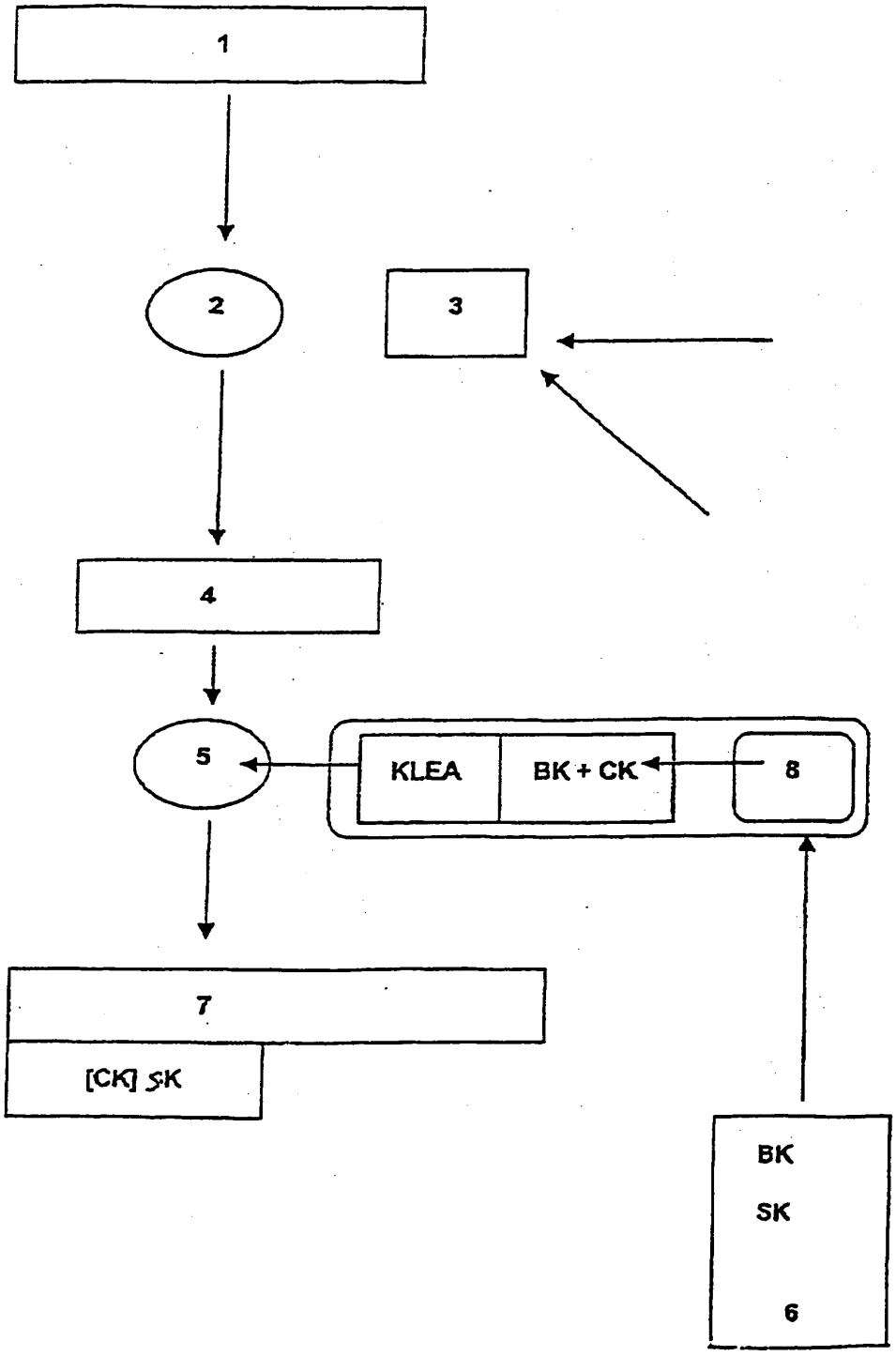
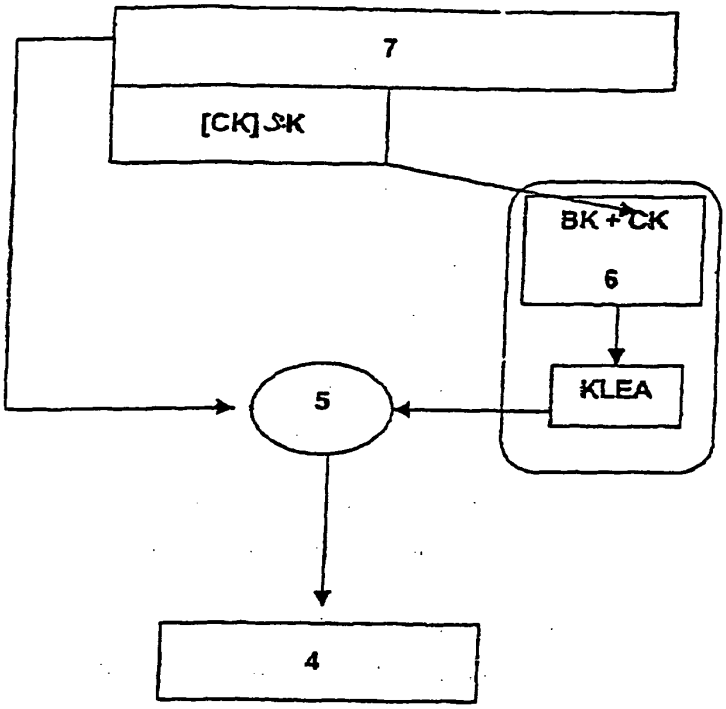


FIG. 2



(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
6 février 2003 (06.02.2003)

PCT

(10) Numéro de publication internationale
WO 03/010722 A3

(51) Classification internationale des brevets[7] :
G11B 20/00, H04N 5/913

(21) Numéro de la demande internationale :
PCT/EP02/08207

(22) Date de dépôt international : 23 juillet 2002 (23.07.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
101 35 888.1 24 juillet 2001 (24.07.2001) DE

(71) Déposant *(pour tous les États désignés sauf US)* : SCM MICROSYSTEMS GMBH [DE/DE]; Oskar-Messter-Strasse 13, 85737 Ismaning (DE).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : LOISEL, Yann [FR/FR]; Lotissement La Revestin, Chemin des Severiers, F-13600 La Ciotat (FR).

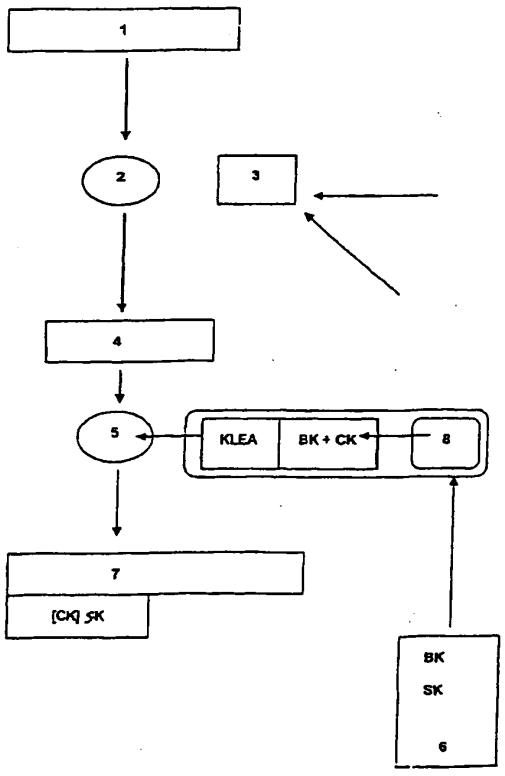
(74) Mandataire : DEGWERT, Hartmut; Prinz & Partner, Manzingerweg 7, 81241 München (DE).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,

[Suite sur la page suivante]

(54) Title: METHOD FOR LOCAL RECORDING OF TELEVISION DIGITAL DATA

(54) Titre : PROCEDE D'ENREGISTREMENT LOCAL DE DONNEES NUMERIQUES POUR LA TELEVISION



(57) Abstract: The invention concerns a method for local recording of digital data received by a transmission network, which consists in encrypting the digital data received with a local recording key (KLEA) and in locally storing the encrypted data (7). The method is characterised in that it comprises the following steps: generating a content key (CK), combining the content key (CK) and a base key (BK) to obtain the local recording key (KLEA), jointly storing the content key (CK) and the encrypted data (7) with the local recording key (KLEA). The invention is particularly applicable to local recording of digital data derived from digital television broadcasting.

(57) Abrégé : La présente invention concerne un procédé d'enregistrement local de données numériques reçues par un réseau de transmission, dans lequel on crypte les données numériques reçues avec une clé locale d'enregistrement (KLEA) et on stocke localement les données cryptées (7). Selon ce procédé, on effectue les étapes suivantes: on génère une clé de contenu (CK), on combine la clé de contenu (CK) et une clé de base (BK) pour obtenir la clé locale d'enregistrement (KLEA), on stocke conjointement la clé de contenu (CK) et les données cryptées (7) avec la clé locale d'enregistrement (KLEA).L'invention s'appliquera tout particulièrement à l'enregistrement local de données issues de diffusion de télévision numérique.

WO 03/010722 A3

LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

(88) **Date de publication du rapport de recherche internationale:** 17 avril 2003

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/08207

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 H04N5/913

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B H04N G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 936 812 A (CANAL PLUS SA) 18 August 1999 (1999-08-18) cited in the application the whole document ---	1-9
A	WO 00 22777 A (MITSUBISHI CORP ;SAITO MAKOTO (JP)) 20 April 2000 (2000-04-20) abstract; figures 1-3 ---	1,7-9
P,A	& EP 1 122 910 A (MITSUBISHI) 8 August 2001 (2001-08-08) page 3, line 53 -page 8, line 21 ---	1,7-9
A	DE 199 23 250 A (BETA RES GMBH) 23 November 2000 (2000-11-23) claim 1 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 January 2003	06/02/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Brunet, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ›nal Application No
PCT/EP 02/08207

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 732 537 A (CANAL PLUS SA) 4 October 1996 (1996-10-04) cited in the application page 7, line 7 -page 8, line 16	1
A	EP 0 912 052 A (CANAL PLUS SA) 28 April 1999 (1999-04-28) claim 1	1
A	US 5 923 754 A (DRISCOLL DANIEL J ET AL) 13 July 1999 (1999-07-13) claim 12	1
A	WO 00 79368 A (BRODIA GROUP) 28 December 2000 (2000-12-28) page 9, line 10 -page 10, line 10	1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int nal Application No
PCT/EP 02/08207

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0936812 A	18-08-1999	EP 0936774 A1	18-08-1999
		EP 0936812 A1	18-08-1999
		AT 225999 T	15-10-2002
		AU 754015 B2	31-10-2002
		AU 2295199 A	30-08-1999
		BR 9907878 A	31-10-2000
		CA 2318992 A1	19-08-1999
		CN 1296695 T	23-05-2001
		DE 69903408 D1	14-11-2002
		EP 1057332 A1	06-12-2000
		HR 20000487 A1	28-02-2001
		HU 0100651 A2	28-06-2001
		WO 9941907 A1	19-08-1999
		JP 2002514834 T	21-05-2002
		NO 20004063 A	13-10-2000
		PL 342260 A1	04-06-2001
		TR 200002348 T2	21-12-2000
		AU 749013 B2	13-06-2002
		AU 2296499 A	30-08-1999
		BR 9907877 A	31-10-2000
		CA 2318879 A1	19-08-1999
		CN 1305674 T	25-07-2001
		EP 1055305 A1	29-11-2000
		HR 20000486 A1	28-02-2001
		HU 0101456 A2	28-09-2001
		WO 9941874 A1	19-08-1999
		JP 2002503919 T	05-02-2002
		NO 20004062 A	13-10-2000
		PL 342261 A1	04-06-2001
		TR 200002350 T2	22-01-2001
		ZA 9901122 A	30-09-1999
		ZA 9901123 A	12-08-1999
WO 0022777 A	20-04-2000	JP 2002101089 A	05-04-2002
		AU 6123599 A	01-05-2000
		CN 1330819 T	09-01-2002
		EP 1122910 A1	08-08-2001
		WO 0022777 A1	20-04-2000
DE 19923250 A	23-11-2000	DE 19923250 A1	23-11-2000
FR 2732537 A	04-10-1996	FR 2732537 A1	04-10-1996
EP 0912052 A	28-04-1999	EP 0912052 A1	28-04-1999
		AU 749106 B2	20-06-2002
		AU 9092698 A	12-04-1999
		BR 9812519 A	25-07-2000
		CA 2304142 A1	01-04-1999
		CN 1279861 T	10-01-2001
		EP 1018265 A1	12-07-2000
		HR 20000146 A1	31-08-2000
		HU 0004368 A2	28-03-2001
		WO 9916244 A1	01-04-1999
		JP 2001517901 T	09-10-2001
		NO 20001529 A	25-05-2000
		PL 339456 A1	18-12-2000
		TR 200000776 T2	21-07-2000
		US 2002048367 A1	25-04-2002

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONAL SEARCH REPORT

Int ›nal Application No
PCT/EP 02/08207

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0912052 A		ZA 9808703 A	01-04-1999
US 5923754 A	13-07-1999	NONE	
WO 0079368 A	28-12-2000	AU 5634100 A	09-01-2001
		WO 0079368 A1	28-12-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

De ge internationale No
PCT/EP 02/08207

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G11B20/00 H04N5/913

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G11B H04N G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 936 812 A (CANAL PLUS SA) 18 août 1999 (1999-08-18) cité dans la demande le document en entier	1-9
A	WO 00 22777 A (MITSUBISHI CORP ;SAITO MAKOTO (JP)) 20 avril 2000 (2000-04-20) abrégé; figures 1-3	1,7-9
P,A	& EP 1 122 910 A (MITSUBISHI) 8 août 2001 (2001-08-08) page 3, ligne 53 -page 8, ligne 21	1,7-9
A	DE 199 23 250 A (BETA RES GMBH) 23 novembre 2000 (2000-11-23) revendication 1	1

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
30 janvier 2003	06/02/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Brunet, L

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

ISDOCID: <WO 03010722A3 I >

IPR2025-00305
ASUS EX1002 Page 205

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP 02/08207

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	FR 2 732 537 A (CANAL PLUS SA) 4 octobre 1996 (1996-10-04) cité dans la demande page 7, ligne 7 -page 8, ligne 16	1
A	EP 0 912 052 A (CANAL PLUS SA) 28 avril 1999 (1999-04-28) revendication 1	1
A	US 5 923 754 A (DRISCOLL DANIEL J ET AL) 13 juillet 1999 (1999-07-13) revendication 12	1
A	WO 00 79368 A (BRODIA GROUP) 28 décembre 2000 (2000-12-28) page 9, ligne 10 -page 10, ligne 10	1

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP 02/08207

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0936812	A	18-08-1999	EP	0936774 A1	18-08-1999
			EP	0936812 A1	18-08-1999
			AT	225999 T	15-10-2002
			AU	754015 B2	31-10-2002
			AU	2295199 A	30-08-1999
			BR	9907878 A	31-10-2000
			CA	2318992 A1	19-08-1999
			CN	1296695 T	23-05-2001
			DE	69903408 D1	14-11-2002
			EP	1057332 A1	06-12-2000
			HR	20000487 A1	28-02-2001
			HU	0100651 A2	28-06-2001
			WO	9941907 A1	19-08-1999
			JP	2002514834 T	21-05-2002
			NO	20004063 A	13-10-2000
			PL	342260 A1	04-06-2001
			TR	200002348 T2	21-12-2000
			AU	749013 B2	13-06-2002
			AU	2296499 A	30-08-1999
			BR	9907877 A	31-10-2000
			CA	2318879 A1	19-08-1999
			CN	1305674 T	25-07-2001
			EP	1055305 A1	29-11-2000
			HR	20000486 A1	28-02-2001
			HU	0101456 A2	28-09-2001
			WO	9941874 A1	19-08-1999
			JP	2002503919 T	05-02-2002
			NO	20004062 A	13-10-2000
			PL	342261 A1	04-06-2001
			TR	200002350 T2	22-01-2001
			ZA	9901122 A	30-09-1999
			ZA	9901123 A	12-08-1999
WO 0022777	A	20-04-2000	JP	2002101089 A	05-04-2002
			AU	6123599 A	01-05-2000
			CN	1330819 T	09-01-2002
			EP	1122910 A1	08-08-2001
			WO	0022777 A1	20-04-2000
DE 19923250	A	23-11-2000	DE	19923250 A1	23-11-2000
FR 2732537	A	04-10-1996	FR	2732537 A1	04-10-1996
EP 0912052	A	28-04-1999	EP	0912052 A1	28-04-1999
			AU	749106 B2	20-06-2002
			AU	9092698 A	12-04-1999
			BR	9812519 A	25-07-2000
			CA	2304142 A1	01-04-1999
			CN	1279861 T	10-01-2001
			EP	1018265 A1	12-07-2000
			HR	20000146 A1	31-08-2000
			HU	0004368 A2	28-03-2001
			WO	9916244 A1	01-04-1999
			JP	2001517901 T	09-10-2001
			NO	20001529 A	25-05-2000
			PL	339456 A1	18-12-2000
			TR	200000776 T2	21-07-2000
			US	2002048367 A1	25-04-2002

Formulaire PCT/ISA/210 (annexe familles de brevets) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

De e internationale No
PCT/EP 02/08207

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0912052	A		ZA	9808703 A	01-04-1999
US 5923754	A	13-07-1999	AUCUN		
WO 0079368	A	28-12-2000	AU	5634100 A	09-01-2001
			WO	0079368 A1	28-12-2000

Formulaire PCT/ISA/210 (annexe familles de brevets) (juillet 1992)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 858 184 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.08.1998 Bulletin 1998/33

(51) Int Cl.[6]: **H04L 9/00**, H04N 5/76

(21) Application number: **98300596.8**

(22) Date of filing: **28.01.1998**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **07.02.1997 IL 12017497**
03.12.1997 GB 9725557

(71) Applicant: **NDS LIMITED**
West Drayton, Middlesex UB7 ODQ (GB)

(72) Inventor: **Tsuria, Yossef**
Shoham 73142 (IL)

(74) Representative: **Hillier, Peter et al**
Reginald W. Barker & Co.,
Chancery House,
53-64, Chancery Lane
London, WC2A 1QU (GB)

(54) Digital recording protection system

(57) A system for producing an output scrambled digital data stream from an input scrambled digital data stream. The input scrambled digital data stream includes a plurality of control messages (ECMs), each ECM including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key. The input scrambled digital data stream also includes a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM. A method for producing the output scrambled digital data stream includes replacing each of the plurality of ECMs with a corresponding transformed ECM (TECM) each corresponding TECM comprising coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key, thus producing the output scrambled digital data stream, wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

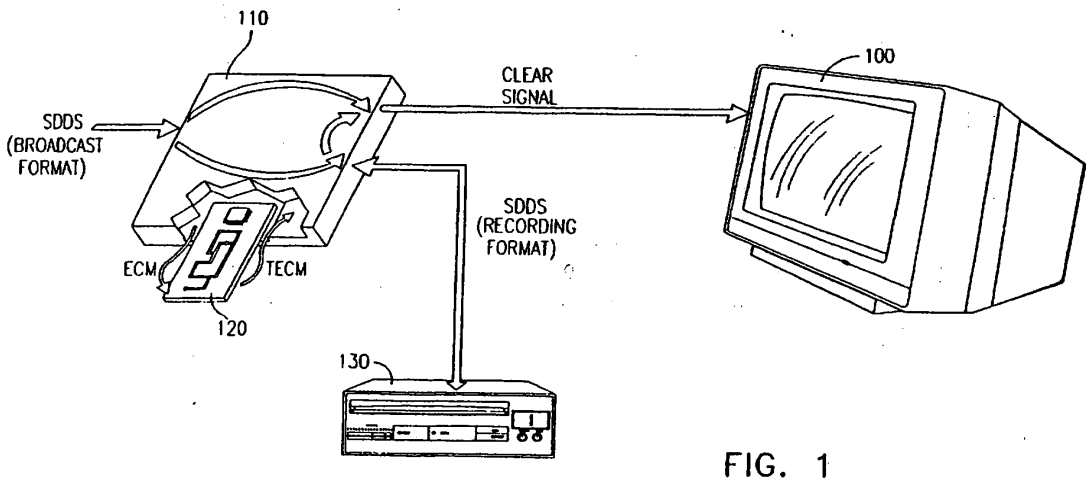


FIG. 1

EP 0 858 184 A2

Printed by Jouve, 75001 PARIS (FR)

Description

FIELD OF THE INVENTION

The present invention relates to the production and recording of digital data streams, particularly scrambled digital data streams such as scrambled digital television data streams.

BACKGROUND OF THE INVENTION

Systems for scrambling a television data stream are well-known in the art. One such system is described in the following US Patents: 5,282,249 to Cohen et al.; 5,481,609 to Cohen et al. Scrambled television data streams described in the Cohen et al. patents comprise both scrambled data representing television signals and coded control messages, also known as ECMs. The ECMs of Cohen et al. comprise, in a coded form, data necessary for generating a control word (CW) which may be used to descramble the scrambled data representing television signals.

While the two patents to Cohen et al. describe an analog system, that is, a system in which analog television data streams are broadcast to television sets, it is appreciated that similar ECM methods may also be used for digital television data streams. Generally, the scrambling techniques used for scrambling analog television signals such as, for example, the well-known "cut-and-rotate" technique, are chosen for their applicability to analog signals. In scrambling of digital television signals other scrambling techniques, well-known in the art, are used, the techniques being more appropriate to digital signals such as, for example, applying the well-known DES algorithm to the digital television signals.

Methods of transmitting a scrambled digital signal, including ECMs, are described in the MPEG-2 standard, ISO/IEC 13818-6, 12 July 1996 and subsequent editions.

Recording of analog television signals such as, for example, recording using a VCR, is well-known in the art and VCR equipment is widely commercially available from a variety of manufacturers. Recording of digital television signals is also known. A consumer digital VCR is described, for example, in the article "A Consumer Digital VCR for Digital Broadcasting" by Okamoto et al., published in IEEE Transactions on Consumer Electronics, Vol. 41, No. 3, August 1995, pp. 643 - 649.

US Patent 5,574,787 to Ryan describes an apparatus and method for copy protection for video platforms in which a specially adapted video recorder, playback device, or set top decoder is used to protect copyright material.

European patent application EP 0 714 204 A2, assigned to LG Electronics, Inc., describes a method for copy protection in digital video systems.

The disclosures of all references mentioned above and throughout the present specification are hereby incorporated herein by reference.

SUMMARY OF THE INVENTION

The present invention seeks to provide an improved system for producing and recording digital data streams, and particularly for protecting recorded digital data streams including digital television data.

The prior art digital recording systems referred to above do not fully address the problem of recording a scrambled digital data stream. The term "digital data stream", as used throughout the present specification and claims, refers in a broad sense to any stream of digital data transmitted continuously at least during a particular period of time, and particularly includes broadcast digital data such as broadcast digital television signals. The term "scrambling" in all of its forms, as used throughout the present specification and claims, refers to any method of scrambling, encoding, or encrypting data, many such methods being well-known in the art.

A digital VCR such as that described by Okamoto et al. records and reproduces a digital bit stream; that is, the digital VCR of Okamoto et al. records and produces whatever bits are presented thereto. Thus, the digital VCR of Okamoto et al. could record and reproduce a scrambled digital data stream. In the system of Okamoto et al., however, problems could arise in descrambling the recorded data stream such as, for example, for playing on a television.

As is well known in the art, security functions in scrambled television systems are typically controlled by a removable security element such as a removable smart card. Furthermore, it is well known in the art that, in actual practice, operators of scrambled television systems periodically replace the removable security elements found in consumer home systems in order to change the security and scrambling behavior of the system.

After replacement of the removable security element or, typically, after a limited transition period following replacement of the removable security element, broadcasts scrambled with methods applicable to the previous removable security element can not be descrambled using the present removable security element. Typically, therefore, if a recording were made on a system such as that described by Okamoto et al. of a broadcast from a digital system using techniques similar to those described by Cohen et al. and in the MPEG-2 standard, both referred to above, the recording would become unusable as soon as a change of removable security elements was carried out by the scrambled television system operator. The present invention seeks to provide apparatus and methods for recording digital data streams which, in addition to having other features, overcome the problem of unusability of recordings after a change of removable security elements.

There is thus provided in accordance with a preferred embodiment of the present invention a method

EX1002 - Page 210
IPR2025-00305
ASUS EX1002 Page 210

for producing an output scrambled digital data stream from an input scrambled digital data stream, the input scrambled digital data stream including a plurality of control messages (ECMs), each ECM including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, the input scrambled digital data stream also including a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the method including replacing each of the plurality of ECMs with a corresponding transformed ECM (TECM), each corresponding TECM including coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key, thus producing the output scrambled digital data stream, wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

Further in accordance with a preferred embodiment of the present invention the step of replacing includes performing the following steps iteratively for each one of the plurality of ECMs: receiving the one ECM and the segment of scrambled digital data associated therewith, generating the associated CW from the one ECM using the ECM key, generating a transformed ECM (TECM) including coded information for generating the associated CW and being encoded using a TECM key, outputting the TECM, and outputting the segment of scrambled digital data associated with the ECM.

There is also provided in accordance with another preferred embodiment of the present invention a method for recording, on a recording medium, a broadcast scrambled digital data stream to produce a scrambled digital recording, the broadcast scrambled digital data stream including a plurality of control messages (ECMs), each ECM including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, the broadcast scrambled digital data stream also including a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the method including receiving the broadcast scrambled digital data stream, and recording on the recording medium a scrambled digital data stream including a plurality of transformed ECMs (TECMs) and the plurality of segments of digital data, wherein each of the plurality of ECMs is replaced with a corresponding TECM, each corresponding TECM including coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key.

Further in accordance with a preferred embodiment of the present invention the recording step includes performing the following steps iteratively for each one of the plurality of ECMs in the broadcast scrambled digital data stream: generating the associated CW from the one ECM using the ECM key, generating a TECM including coded information for generating the associated CW and being encoded using a TECM key, recording the TECM on the recording medium, and recording the segment of scrambled digital data associated with the one ECM on the recording medium.

Still further in accordance with a preferred embodiment of the present invention the recording medium includes a digital tape.

Further in accordance with a preferred embodiment of the present invention the recording medium includes a computer-accessible storage medium associated with a computer.

Additionally in accordance with a preferred embodiment of the present invention the broadcast scrambled digital data stream includes a television scrambled digital data stream.

Moreover in accordance with a preferred embodiment of the present invention each of the plurality of ECMs is encoded using a hashing method.

There is also provided in accordance with another preferred embodiment of the present invention apparatus for recording, on a recording medium, a broadcast scrambled digital data stream to produce a recorded scrambled digital data stream, the broadcast scrambled digital data stream including a plurality of scrambling control messages (ECMs), each ECM including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, and a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the apparatus including receiving apparatus for receiving the broadcast scrambled digital data stream, and recording apparatus for recording on the recording medium a scrambled digital data stream including a plurality of transformed ECMs (TECMs) and the plurality of segments of digital data, wherein each of the plurality of ECMs is replaced with a corresponding TECM, each corresponding TECM including coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key.

There is also provided in accordance with another preferred embodiment of the present invention apparatus for producing an output scrambled digital data stream from an input scrambled digital data stream, the input scrambled digital data stream including a plurality of scrambling control messages (ECMs), each ECM including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, and a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the apparatus including ECM replacement apparatus for replacing each of the plurality of ECMs with a

EP0858184A2_I_>

EX1002 - Page 211

IPR2025-00305
ASUS EX1002 Page 211

corresponding transformed ECM (TECM), each corresponding TECM including coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key, wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

Further in accordance with a preferred embodiment of the present invention the recording apparatus includes a CW extractor for generating the associated CW from each of the plurality of ECMs using the ECM key, a TECM generator for receiving the associated CW from the CW extractor and for generating a TECM including coded information for generating the associated CW and being encoded using a TECM key, and medium recording apparatus for receiving the TECM from the TECM generator and the segment of scrambled digital data from the receiving apparatus and for recording the TECM and the segment of scrambled digital data associated with the one of the plurality of ECMs on the recording medium.

Still further in accordance with a preferred embodiment of the present invention the ECM replacement apparatus includes a CW extractor for generating the associated CW from each of the plurality of ECMs using the ECM key, and a TECM generator for receiving the associated CW from the CW extractor and for generating a TECM including coded information for generating the associated CW and encoded using a TECM key.

Additionally in accordance with a preferred embodiment of the present invention the apparatus includes a removable security device, wherein the removable security device includes the CW extractor.

Moreover in accordance with a preferred embodiment of the present invention the removable security device also includes the TECM generator.

Further in accordance with a preferred embodiment of the present invention the removable security device includes a smart card.

There is also provided in accordance with another preferred embodiment of the present invention apparatus for transforming a scrambling control message (ECM) including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key into a transformed scrambling control message (TECM), the apparatus including ECM input apparatus for receiving the ECM, a CW extractor for generating the associated CW from the ECM using the ECM key, a TECM generator for generating a transformed ECM (TECM) including coded information for generating the associated CW and being encoded using a TECM key, and ECM output apparatus for outputting the TECM, wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM change time.

There is also provided in accordance with another preferred embodiment of the present invention apparatus for producing an output scrambled digital data stream from an input scrambled digital data stream, the input scrambled digital data stream including a plurality of control messages (ECMs), each ECM including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, the input scrambled digital data stream also including a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the apparatus including scrambled digital data stream input apparatus for receiving an ECM and a segment of scrambled digital data associated therewith, ECM replacement apparatus for replacing the ECM with a transformed ECM (TECM), and scrambled digital data stream output apparatus for outputting the output scrambled digital data stream including the TECM and the segment of scrambled digital data, wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

Further in accordance with a preferred embodiment of the present invention the apparatus includes ECM interface apparatus for outputting the ECM and receiving the TECM.

Still further in accordance with a preferred embodiment of the present invention the ECM interface is adapted to receive a removable security element.

Additionally in accordance with a preferred embodiment of the present invention the removable security element includes a smart card.

There is also provided in accordance with another preferred embodiment of the present invention a method for transforming a scrambling control message (ECM) including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key into a transformed scrambling control message (TECM), the method including receiving the ECM, generating the associated CW from the ECM using the ECM key, generating a transformed ECM (TECM) including coded information for generating the associated CW and being encoded using a TECM key, and outputting the TECM, wherein the ECM key is replaced with a new ECM key at an ECM change time, and the TECM key is not replaced at the ECM change time.

There is also provided in accordance with another preferred embodiment of the present invention a method for producing an output scrambled digital data stream from an input scrambled digital data stream, the input scrambled digital data stream including a plurality of control messages (ECMs), each ECM including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, the input scrambled digital data stream also including a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scram-

EX1002 - Page 212
IPR2025-00305
ASUS EX1002 Page 212

bled using the CW associated with the ECM, the method including receiving an ECM and a segment of scrambled digital data associated therewith, replacing the ECM with a transformed ECM (TECM), and outputting the output scrambled digital data stream including the TECM and the segment of scrambled digital data, wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

Further in accordance with a preferred embodiment of the present invention the method also includes outputting the ECM and receiving the TECM.

Still further in accordance with a preferred embodiment of the present invention the step of outputting the ECM and receiving the TECM includes outputting the ECM to a removable security element and receiving the TECM from the removable security element.

Additionally in accordance with a preferred embodiment of the present invention removable security element includes a smart card.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified partly pictorial, partly block-diagram illustration of a scrambled digital data stream recording and playback system, constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2 is a simplified block diagram illustrating the production of a recording scrambled digital data stream from a broadcast scrambled digital data stream by a portion of the apparatus of Fig. 1;

Fig. 3 is a simplified block diagram illustration of a portion of the apparatus of Fig. 1;

Fig. 4 is a simplified flowchart illustration of a preferred method of operation of the apparatus of Fig. 3; and

Fig. 5 is a simplified flowchart illustration of a preferred implementation of step 210 of Fig. 4.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Reference is now made to Fig. 1 which is a simplified partly pictorial, partly block-diagram illustration of a scrambled digital data stream (SDDS) recording and playback system, constructed and operative in accordance with a preferred embodiment of the present invention. The system of Fig. 1 comprises a television set 100. The television set 100 may comprise any appropriate commercially available television set. As described below, in accordance with the other elements of the system Fig. 1 described below, the television set 100 may comprise either an appropriate analog television set or an appropriate digital television set.

The system of Fig. 1 also comprises an integrated receiver-decoder (IRD) 110. The IRD 110 may be based on any appropriate commercially-available IRD operative to receive and decode a scrambled broadcast digital data stream and preferably additionally contains other hardware and/or software components, as described below.

The system of Fig. 1 also comprises a removable security element, such as a smart card 120, in removable operative attachment with the IRD 110. The smart card 120 is typically suitably programmed, as is well-known in the art, to provide control words (CWs) for descrambling of a scrambled broadcast digital data stream by the IRD 110. Methods for programming and utilizing smart cards such as the smart card 120 to produce CWs are well-known in the art and are described, for example, in US Patents 5,282,249 to Cohen et al. and 5,481,609 to Cohen et al., referred to above, with suitable modifications, as are well-known in the art and described above, particularly in the MPEG-2 standard, for operating on digital rather than on analog data.

The system of Fig. 1 also preferably comprises a digital VCR 130, which may comprise any suitable digital VCR such as, for example, the digital VCR described in the article "A Consumer Digital VCR for Digital Broadcasting" by Okamoto et al., referred to above. It is appreciated that any other appropriate digital recording apparatus may be used in place of the digital VCR 130, the digital VCR 130 being shown in Fig. 1 by way of example only. For example, and without limiting the generality of the foregoing, an appropriate computer system may be used in place of the digital VCR 130, the computer system being typically operative to record onto a computer-accessible storage medium associated therewith.

The IRD 110 is preferably operatively attached to the television set 100 and the digital VCR 130. It is appreciated that the IRD 110 may include digital-to-analog conversion apparatus (not shown), as is well known in the art, and may provide analog signals to the television set 100, in which case the television set 100 may comprise an analog television set. Alternatively, the IRD 110 may provide digital signals to the television set 100, in which case the television set 100 may comprise a digital television set. In any case, it is appreciated that digital signals are preferably used between the IRD 110 and the digital VCR 130.

The operation of the system of Fig. 1 is now briefly described. The IRD 110 receives a scrambled digital data stream, also known herein as a SDDS, from a broadcast source. The broadcast source may comprise any appropriate broadcast source such as, for example, a digital cable broadcast, a local digital television broadcast, or a digital satellite television broadcast, all of which are well-known in the art. Typically, the SDDS may comprise an MPEG-2 data stream, as described in the MPEG-2 standard, referred to above. More gener-

EDOCID: <EP_____0858184A2_I_>

IPR2025-00305
ASUS EX1002 Page 213

ally, it is appreciated that the present invention is not limited to television broadcasts, but is applicable to all types of digital broadcast, including data broadcasts, so that the broadcast source may comprise any appropriate source broadcasting a SDDS in appropriate format.

The IRD 110, in cooperation with the smart card 120, is preferably operative to descramble the SDDS. Typically, as is well known in the art and as is described above, the SDDS comprises a plurality of ECMs. Each ECM is associated with, and is typically followed by, a scrambled digital data segment (SDSEG). Each ECM is typically encoded and comprises therein information, such as a seed, which can be used, typically by the smart card 120, to generate a CW, the CW in turn being utilizable to unscramble the associated SDSEG.

It is appreciated that many different methods may be used to imbed the seed in the ECM and that corresponding methods can be used to extract the seed therefrom and to generate the CW. For example and without limiting the generality of the foregoing, the seed may be the input to a one-way function such as a hash function, and the CW may be the result of performing the hash function on the seed. The CW, in turn, can be used, typically by the IRD 110, as a key for descrambling the scrambled data segment associated with the ECM.

Reference is now additionally made to Fig. 2, which is a simplified block diagram illustrating the production of a recording scrambled digital data stream from a broadcast scrambled digital data stream by the IRD 110 of Fig. 1. The block diagram of Fig. 2 comprises a simplified illustration of a broadcast SDDS 140, which, as described above, typically comprises a plurality of ECMs and a plurality of associated SDSEGs, such as: an nth ECM 145; an nth SDSEG 150 associated with the nth ECM 145; and n+1th ECM 155; and an n+1th SDSEG 160 associated with the n+1th ECM 155. It is appreciated that the block diagram of Fig. 2 is schematic only, and that the plurality of ECMs and the plurality of associated SDSEGs need not be physically contiguous. One particular example of the actual layout of ECMs and the associated SDSEGs in an SDDS is given in the MPEG-2 standard, referred to above.

The IRD 110 of Fig. 1, in cooperation with the smart card 120, is preferably operative to process the broadcast SDDS 140, in order to produce a recording SDDS 165, as follows. Each ECM, such as the nth ECM 145, is processed as described above, typically using an ECM key, which may comprise a one-way function as described above, the ECM key being known to the smart card 120, in order to obtain the associated CW such as an nth CW 170. The nth CW 170 is then processed using another key, referred to throughout the present specification and claims as a TECM key, in order to produce an nth TECM 175 which may later be used, with the TECM key, to generate the nth CW 170.

Preferably each TECM, such as, for example, the nth TECM 175, is also signed with an appropriate digital signature, as is well known in the art. Preferably, each TECM key is associated with a unique digital signature. Preferably, upon subsequent playback and descrambling of the recording SDDS 165 the digital signature is checked, and only a valid digital signature indicating that the recording SDDS 165 was produced with the apparatus of Fig. 1, typically particularly with the smart card 120 of Fig. 1, will be descrambled by the apparatus of Fig. 1. The use of such a digital signature is considered preferable in order to discourage unauthorized duplication and subsequent playback of the recording SDDS 165 using apparatus other than the apparatus of Fig. 1, particularly using a different smart card at some other location in place of the smart card 120.

The TECM key may be of similar type to the ECM key such as, for example, a one-way function. The TECM key, however, is preferably permanently associated with the system of Fig. 1; particularly, the TECM key does not change even when the smart card 120 is replaced by the system operator, as described above. Thus, it will be appreciated that any SDDS associated with the TECM key may still be descrambled using the apparatus of Fig. 1 even after such a replacement of the smart card 120. It is appreciated that the TECM key may be produced in a wide variety of ways, such as, for example, the TECM key may be associated with and, typically, stored in the IRD 110; the smart card 120; a combination of the IRD 110 and the smart card 120, such as partly in the IRD 110 and partly in the smart card 120; or another portion of the system of Fig. 1 (not shown). It is also appreciated that the TECM key may be personal to a particular user of the apparatus of Fig. 1, with more than one TECM key being associated with the apparatus of Fig. 1 and the appropriate TECM key being produced upon identification of a user of the apparatus of Fig. 1 by any method well known in the art, such as by provision of a personal identification number (PIN).

It is appreciated that, in a case where the TECM key is at least partially associated with or stored in a removable security element such as the smart card 120, a method is preferably provided for keeping the TECM key unchanged even when the smart card 120 is replaced, as described above. Methods for providing an unchanging item of information are well known in prior art scrambled television systems using removable security elements. For example, and without limiting the generality of the foregoing, when the smart card 120 is replaced an operation may be carried out whereby an unchanging item of information stored only in the smart card 120 is temporarily stored in the IRD 110 and is then written to the replacement smart card (not shown) and erased from the IRD 110. Such prior art methods, for example, may be used to cause a TECM key to be unchanging even when the smart card 120 is replaced.

After the nth TECM 175 is generated and placed in the recording SDDS 165, the nth SDSEG 150 may be placed in the recording SDDS 165. It is appreciated that the present invention provides an apparatus and method for producing an appropriate recording SDDS 165

EX1002 - Page 214
IPR2025-00305
ASUS EX1002 Page 214

without requiring descrambling of any SDSEG such as the nth SDSEG 150 during the production of the recording SDDS 165 and without requiring a scrambling operation to produce an SDSEG to occur in the system of Fig. 1 at any time.

It is appreciated that the method described above with respect to the nth ECM 145 and the nth SDSEG 150 may be repeatedly or iteratively applied to other ECMs and the associated SDSEGs such as, for example, the n+1th ECM 155, associated with an n+1th CW 177, to produce an n+1th TECM 180 and the n+1th SDSEG 160 in the recording SDDS 165.

It is also appreciated that, during playback of a recording SDDS from the digital VCR 130 through the IRD 110 and associated smart card 120 to the television 100, the IRD 110 and the associated smart card 120 may perform operations similar to those performed on a broadcast SDDS, but using the TECM key rather than the ECM key.

Reference is now made to Fig. 3, which is a simplified block diagram illustration of a portion of the IRD 110 of Fig. 1. The portion of the IRD 110 shown in Fig. 3 is shown for providing a better understanding of the construction and operation of the present invention, with standard components well-known in the art, such as components used to receive a broadcast SDDS, not shown in Fig. 3. It is appreciated that the components shown in Fig. 3 may be provided in hardware or in software and, if provided in software, may be provided in combination in software running on one or more general-purpose or special-purpose processors, as is well-known in the art.

The apparatus of Fig. 3 comprises a descrambler 185 and a control word extractor 190. The control word extractor 190 may preferably operate as described above to extract CWs from ECMs in the SDDS, as described above, and to provide the CWs to the descrambler 185. The descrambler 185 meanwhile receives SDSEGs in the SDDS, as described above, and applies each CW received from the descrambler 185 to the associated SDSEG to produce a clear signal.

In addition, the control word extractor 190 preferably supplies the CWs to a scrambled digital data stream transformer 195, the scrambled digital data stream transformer 195 preferably comprising a TECM generator 200. The scrambled data stream transformer 195 also receives the broadcast SDDS and operates, as described above with reference to Figs. 1 and 2 and below with reference to Figs. 4 and 5, to produce therefrom a recording SDDS, which is typically provided to a recorder.

It may thus be appreciated that descrambling operations to produce a clear signal, the descrambling operations being typically similar to descrambling operations well-known in the art, may occur in the apparatus of Fig. 3 in parallel with the production of a recording SDDS. It is appreciated that, in a preferred implementation of the apparatus of Fig. 3, adequate buffering may be provided in the scrambled digital data stream transformer 195 or elsewhere in order to permit continuous production of the recording SDDS from the broadcast SDDS. Such methods of buffering are well-known in the art.

It is further appreciated that the apparatus of Fig. 3 may be operative to descramble a recording SDDS and provide a clear signal therefrom by providing the recording SDDS as input to the apparatus of Fig. 3 in place of the broadcast SDDS, the control word extractor being operative in such a mode to provide control words, as described above, using a TECM key rather than an ECM key.

Reference is now made to Fig. 4 which is a simplified flowchart illustration of a preferred method of operation of the apparatus of Fig. 3. The method of Fig. 4 preferably comprises the following steps:

An input SDDS is received (step 205). Each ECM in the input SDDS is replaced with a TECM, the ECM comprising CW generating information and the TECM also comprising control word generating information for generating the same CW as the ECM (step 210). An output SDDS is thus produced. The output SDDS is then output (step 215)

Reference is now made to Fig. 5, which is a simplified flowchart illustration of a preferred implementation of step 210 of Fig. 4. The method of Fig. 5 preferably comprises the following steps, which are preferably performed iteratively for each ECM in the input SDDS:

One ECM and an SDSEG associated with the ECM are input (step 220). The CW associated with the ECM is generated from the ECM using an ECM key (step 225). A TECM is generated using a TECM key, the TECM comprising information for generating the same CW as the ECM (step 230). The TECM is output (step 235), and the SDSEG associated with the ECM, and thus also associated with the TECM, is also output (step 240).

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination. It is particularly appreciated that the functions described herein as being performed by a removable security device or smart card may be performed by another appropriate part of the system described, such as an IRD.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only the by claims which follow:

SDOCID: <EP 0858184A2 I >

EX1002 - Page 215
IPR2025-00305
ASUS EX1002 Page 215

Claims

1. A method for producing an output scrambled digital data stream from an input scrambled digital data stream, the input scrambled digital data stream comprising a plurality of control messages (ECMs), each ECM comprising coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, the input scrambled digital data stream also comprising a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the method comprising:

   replacing each of the plurality of ECMs with a corresponding transformed ECM (TECM), each corresponding TECM comprising coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key, thus producing the output scrambled digital data stream,
   wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

2. A method according to claim 1 and wherein the step of replacing comprises performing the following steps iteratively for each one of the plurality of ECMs:

   receiving the one ECM and the segment of scrambled digital data associated therewith;
   generating the associated CW from the one ECM using the ECM key;
   generating a transformed ECM (TECM) comprising coded information for generating the associated CW and being encoded using a TECM key;
   outputting the TECM; and
   outputting the segment of scrambled digital data associated with the ECM.

3. A method for recording, on a recording medium, a broadcast scrambled digital data stream to produce a scrambled digital recording, the broadcast scrambled digital data stream comprising a plurality of control messages (ECMs), each ECM comprising coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, the broadcast scrambled digital data stream, also comprising a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the method comprising:

   receiving the broadcast scrambled digital data stream; and
   recording on the recording medium a scrambled digital data stream comprising a plurality of transformed ECMs (TECMs) and the plurality of segments of digital data, wherein each of the plurality of ECMs is replaced with a corresponding TECM, each corresponding TECM comprising coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key.

4. A method according to claim 3 and wherein the recording step comprises performing the following steps iteratively for each one of the plurality of ECMs in the broadcast scrambled digital data stream:

   generating the associated CW from the one ECM using the ECM key;
   generating a TECM comprising coded information for generating the associated CW and being encoded using a TECM key;
   recording the TECM on the recording medium; and
   recording the segment of scrambled digital data associated with the one ECM on the recording medium.

5. A method according to either claim 3 or claim 4 and wherein the recording medium comprises a digital tape.

6. A method according to either claim 3 or claim 4 and wherein the recording medium comprises a computer-accessible storage medium associated with a computer.

7. A method according to any of claims 3 - 6 and wherein the broadcast scrambled digital data stream comprises a television scrambled digital data stream.

8. A method according to any of the preceding claims and wherein each of the plurality of ECMs is encoded using a hashing method.

9. Apparatus for recording, on a recording medium, a broadcast scrambled digital data stream to produce a recorded scrambled digital data stream, the broadcast scrambled digital data stream comprising a plurality of scrambling control messages (ECMs), each ECM comprising coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, and a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated

EX1002 - Page 216
IPR2025-00305
ASUS EX1002 Page 216

with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the apparatus comprising:

receiving apparatus for receiving the broadcast scrambled digital data stream; and
recording apparatus for recording on the recording medium a scrambled digital data stream comprising a plurality of transformed ECMs (TECMs) and the plurality of segments of digital data, wherein each of the plurality of ECMs is replaced with a corresponding TECM, each corresponding TECM comprising coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key.

10. Apparatus for producing an output scrambled digital data stream from an input scrambled digital data stream, the input scrambled digital data stream comprising a plurality of scrambling control messages (ECMs), each ECM comprising coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, and a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the apparatus comprising:

ECM replacement apparatus for replacing each of the plurality of ECMs with a corresponding transformed ECM (TECM), each corresponding TECM comprising coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key,
wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

11. Apparatus according to claim 9 and wherein the recording apparatus comprises:

a CW extractor for generating the associated CW from each of the plurality of ECMs using the ECM key;
a TECM generator for receiving the associated CW from the CW extractor and for generating a TECM comprising coded information for generating the associated CW and being encoded using a TECM key; and
medium recording apparatus for receiving the TECM from the TECM generator and the segment of scrambled digital data from the receiving apparatus and for recording the TECM and the segment of scrambled digital data associated with the one of the plurality of ECMs on the recording medium.

12. Apparatus according to claim 10 and wherein the ECM replacement apparatus comprises:

a CW extractor for generating the associated CW from each of the plurality of ECMs using the ECM key; and
a TECM generator for receiving the associated CW from the CW extractor and for generating a TECM comprising coded information for generating the associated CW and encoded using a TECM key.

13. Apparatus according to either claim 11 or claim 12 and also comprising a removable security device,

wherein the removable security device comprises the CW extractor.

14. Apparatus according to claim 13 and wherein the removable security device also comprises the TECM generator.

15. Apparatus according to either claim 13 or claim 14 and wherein the removable security device comprises a smart card.

16. Apparatus for transforming a scrambling control message (ECM) comprising coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key into a transformed scrambling control message (TECM), the apparatus comprising:

ECM input apparatus for receiving the ECM;
a CW extractor for generating the associated CW from the ECM using the ECM key;
a TECM generator for generating a transformed ECM (TECM) comprising coded information for generating the associated CW and being encoded using a TECM key; and
ECM output apparatus for outputting the TECM,
wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM change time.

17. Apparatus for producing an output scrambled digital data stream from an input scrambled digital data stream, the input scrambled digital data stream comprising a plurality of control messages (ECMs), each ECM comprising coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, the input scrambled digital data stream also comprising a

ISDOCID: <EP 0858184A2 I >

EX1002 - Page 217
IPR2025-00305
ASUS EX1002 Page 217

plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the apparatus comprising:

scrambled digital data stream input apparatus for receiving an ECM and a segment of scrambled digital data associated therewith;
ECM replacement apparatus for replacing the ECM with a transformed ECM (TECM); and
scrambled digital data stream output apparatus for outputting the output scrambled digital data stream comprising the TECM and the segment of scrambled digital data,
wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

18. Apparatus according to claim 17 and also comprising:

ECM interface apparatus for outputting the ECM and receiving the TECM.

19. Apparatus according to claim 18 and wherein the ECM interface is adapted to receive a removable security element.

20. Apparatus according to claim 19 and wherein the removable security element comprises a smart card.

21. A method for transforming a scrambling control message (ECM) comprising coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key into a transformed scrambling control message (TECM), the method comprising:

receiving the ECM;
generating the associated CW from the ECM using the ECM key;
generating a transformed ECM (TECM) comprising coded information for generating the associated CW and being encoded using a TECM key; and
outputting the TECM,
wherein the ECM key is replaced with a new ECM key at an ECM change time, and the TECM key is not replaced at the ECM change time.

22. A method for producing an output scrambled digital data stream from an input scrambled digital data stream, the input scrambled digital data stream comprising a plurality of control messages (ECMs), each ECM comprising coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key, the input scrambled digital data stream also comprising a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM, the method comprising:

receiving an ECM and a segment of scrambled digital data associated therewith;
replacing the ECM with a transformed ECM (TECM); and
outputting the output scrambled digital data stream comprising the TECM and the segment of scrambled digital data,
wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

23. A method according to claim 22 and also comprising: outputting the ECM and receiving the TECM.

24. A method according to claim 23 and wherein the step of outputting the ECM and receiving the TECM comprises:

outputting the ECM to a removable security element and receiving the TECM from the removable security element

25. A method according to claim 24 and wherein the removable security element comprises a smart card.

EX1002 - Page 218
IPR2025-00305
ASUS EX1002 Page 218

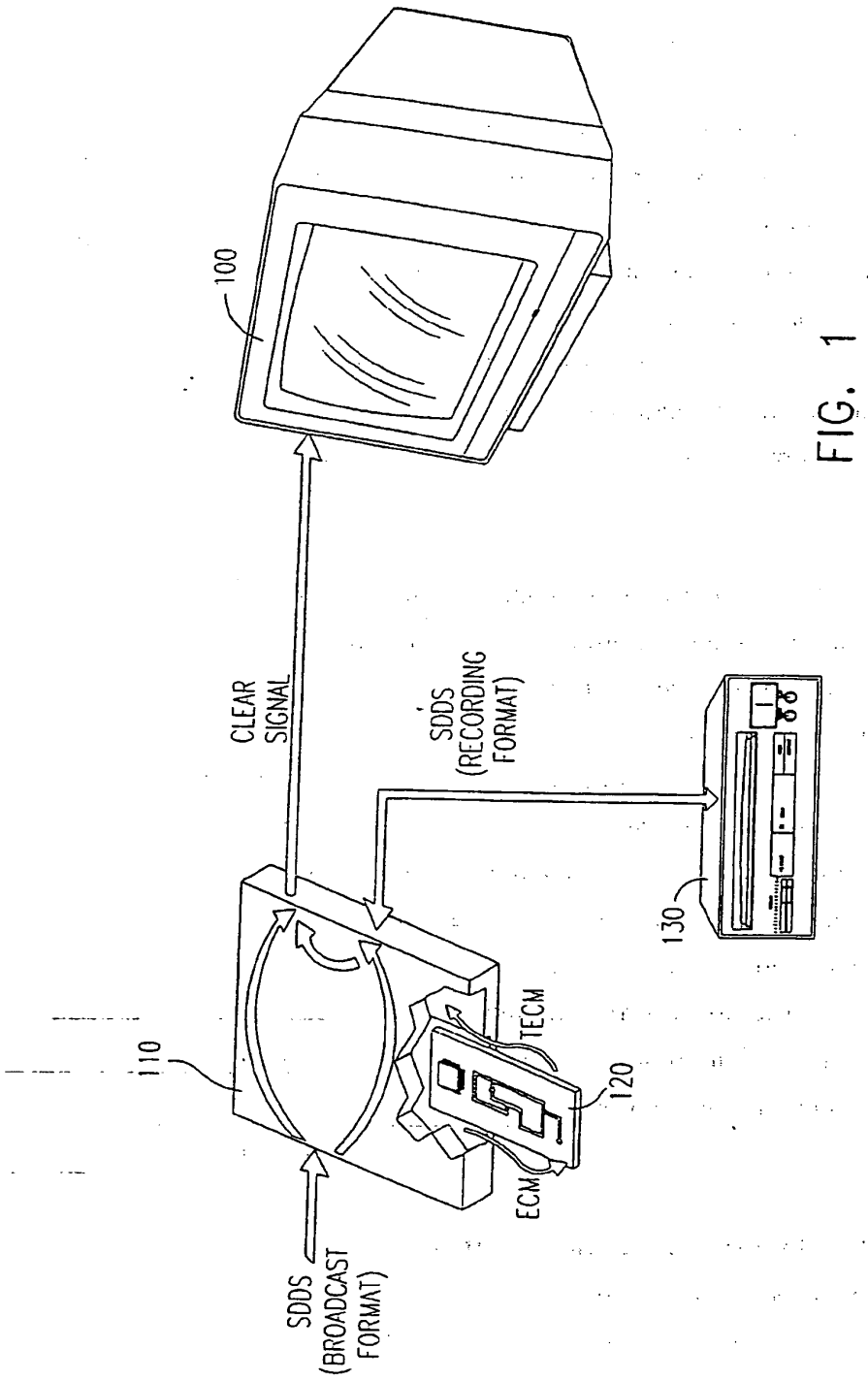


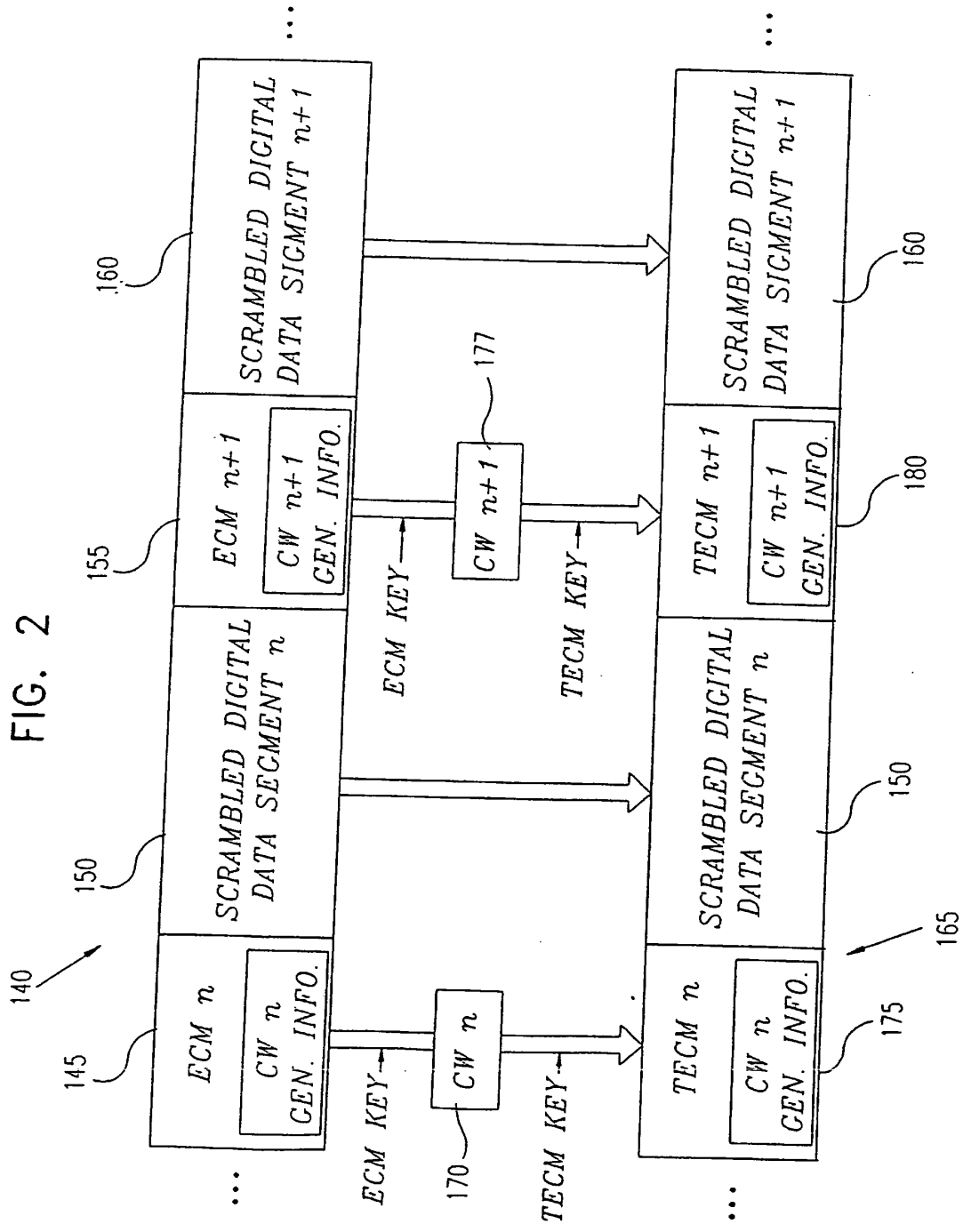
FIG. 1

SDOCID: <EP 0858184A2 I >

EX1002 - Page 219

IPR2025-00305
ASUS EX1002 Page 219

FIG. 2



EX1002 - Page 220
IPR2025-00305
ASUS EX1002 Page 220

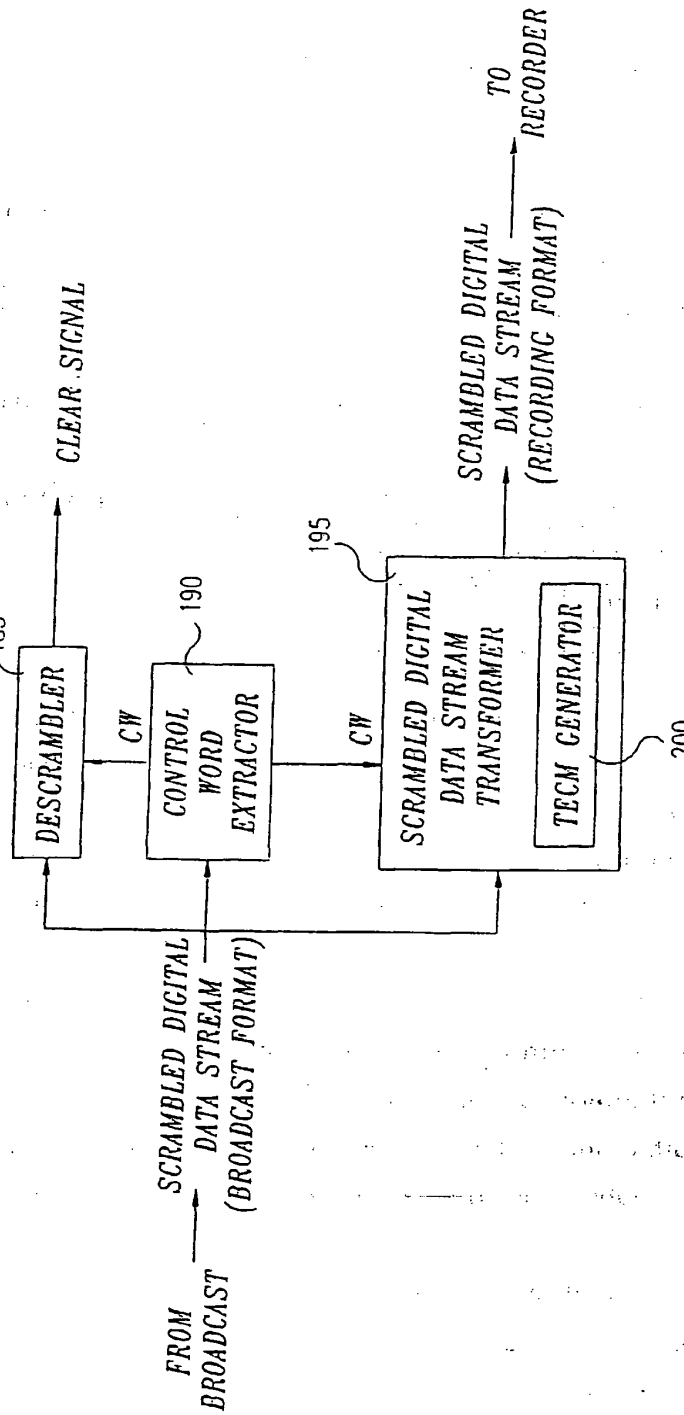


FIG. 3

SDOCID: <EP_____0858184A2_I_>

IPR2025-00305
ASUS EX1002 Page 221

FIG. 4

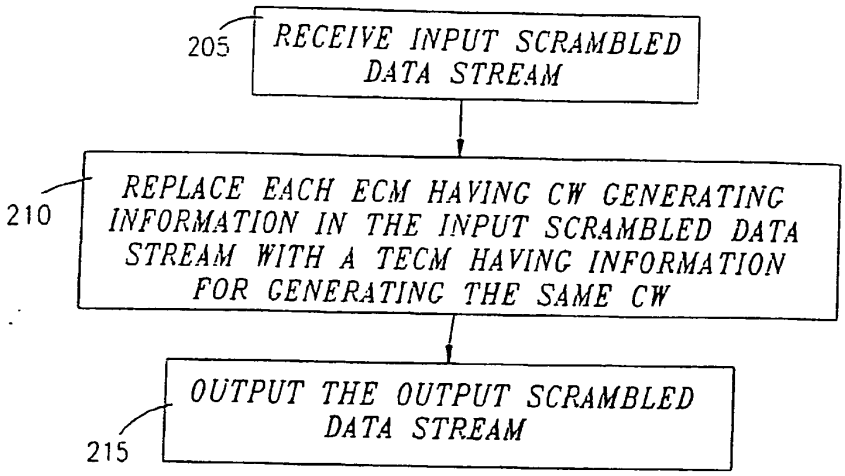
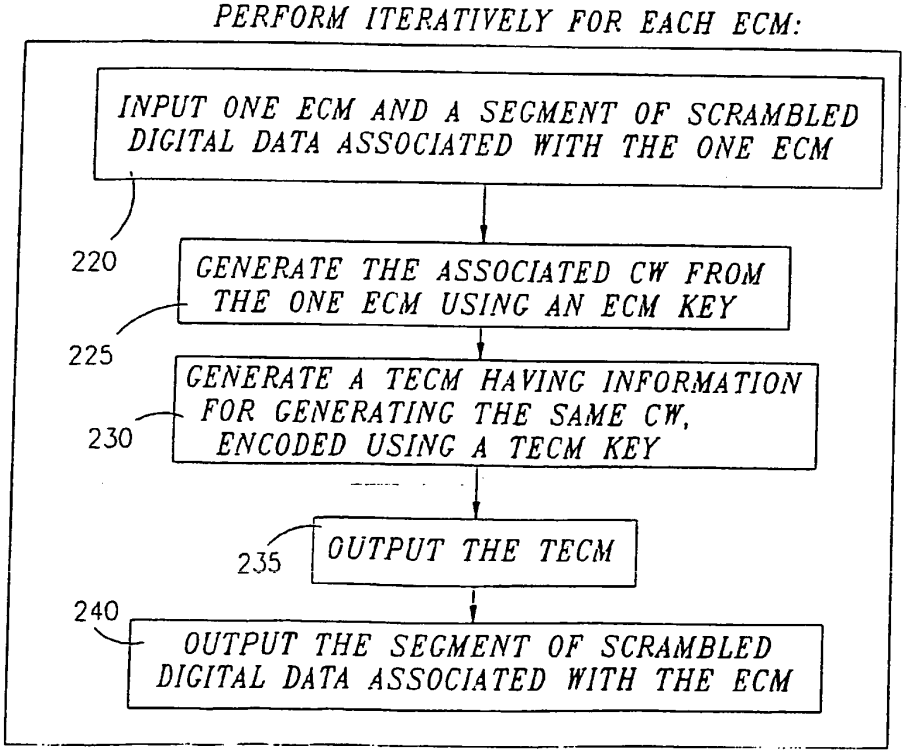


FIG. 5



EX1002 - Page 222
IPR2025-00305
ASUS EX1002 Page 222

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 858 184 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.09.1999 Bulletin 1999/35

(43) Date of publication A2:
12.08.1998 Bulletin 1998/33

(21) Application number: **98300596.8**

(22) Date of filing: **28.01.1998**

(51) Int Cl.[6]: **H04L 9/00**, H04N 5/76, H04N 7/167, H04N 5/913

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **07.02.1997 IL 12017497**
03.12.1997 GB 9725557

(71) Applicant: **NDS LIMITED**
West Drayton, Middlesex UB7 ODQ (GB)

(72) Inventor: **Tsuria, Yossef**
Shoham 73142 (IL)

(74) Representative: **Hillier, Peter et al**
Reginald W. Barker & Co.,
Chancery House,
53-64, Chancery Lane
London, WC2A 1QU (GB)

(54) Digital recording protection system

(57) A system for producing an output scrambled digital data stream from an input scrambled digital data stream. The input scrambled digital data stream includes a plurality of control messages (ECMs), each ECM including coded information for generating a control word (CW) associated with the ECM and being encoded using an ECM key. The input scrambled digital data stream also includes a plurality of segments of scrambled digital data, each segment of scrambled digital data being associated with one of the plurality of ECMs and being scrambled using the CW associated with the ECM. A method for producing the output scrambled digital data stream includes replacing each of the plurality of ECMs with a corresponding transformed ECM (TECM) each corresponding TECM comprising coded information for generating the CW associated with the corresponding ECM and being encoded using a TECM key, thus producing the output scrambled digital data stream, wherein the ECM key is replaced with a new ECM key at an ECM key change time, and the TECM key is not replaced at the ECM key change time.

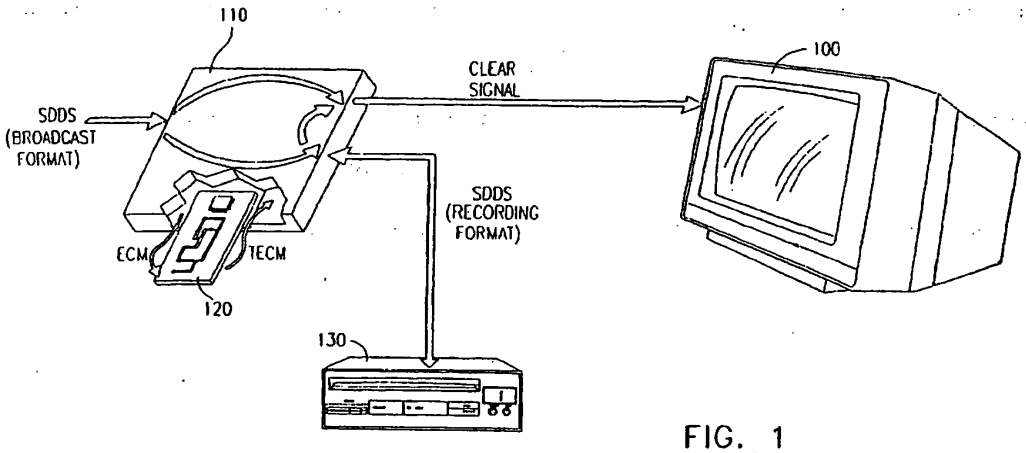


FIG. 1

EP 0 858 184 A3

Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 30 0596

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	FR 2 732 537 A (CANAL PLUS SA) 4 October 1996 (1996-10-04)	1-5,7, 9-12, 16-18, 21-23	H04L9/00 H04N5/76 H04N7/167 H04N5/913
Y	* page 2, line 12 - page 3, line 6 * * page 6, line 10 - line 13 * * page 7, line 25 - page 9, line 4 *	8,13-15, 19,20, 24,25	
Y	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, no. 266, 21 December 1995 (1995-12-21), pages 64-77, XP000559450 ISSN: 0251-0936	13-15, 19,20, 24,25	
A	* page 67, right-hand column, line 4 - line 5 * * page 76, right-hand column, paragraph 8 - page 77, right-hand column, paragraph 4 * * table 7 *	1,3,9, 10,16, 17,21,22	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04N
Y	EP 0 750 423 A (IRDETO BV) 27 December 1996 (1996-12-27) * column 3, line 32 - line 50 *	8	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	9 July 1999	Sindic, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 30 0596

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	GUILLOU L C ET AL: "ENCIPHERMENT AND CONDITIONAL ACCESS" SMPTE JOURNAL, vol. 103, no. 6, 1 June 1994 (1994-06-01), pages 398-406, XP000457575 ISSN: 0036-1682 * page 400, middle column, paragraph 2 * * page 402, left-hand column, paragraph 3 - middle column, paragraph 1 * * page 404, middle column, paragraph 5 - page 406, middle column, paragraph 5 *	13-15, 19,20, 24,25	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	9 July 1999	Sindic, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

EX1002 - Page 225
IPR2025-00305
ASUS EX1002 Page 225

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 30 0596

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-07-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2732537 A	04-10-1996	NONE	
EP 0750423 A	27-12-1996	AU 704421 B	22-04-1999
		AU 5604596 A	09-01-1997
		BR 9602862 A	22-04-1998
		CA 2179223 A	24-12-1996
		CN 1144437 A	05-03-1997
		CZ 9601802 A	11-12-1996
		HU 9601728 A	28-01-1997
		JP 9135435 A	20-05-1997
		NO 962605 A	27-12-1996
		SK 82496 A	03-06-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

IPR2025-00305
ASUS EX1002 Page 226

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 5/913, 7/16

A1

(11) International Publication Number: **WO 00/56068**

(43) International Publication Date: 21 September 2000 (21.09.00)

(21) International Application Number: PCT/US00/06834

(22) International Filing Date: 15 March 2000 (15.03.00)

(30) Priority Data:

60/124,479	15 March 1999 (15.03.99)	US
60/124,480	15 March 1999 (15.03.99)	US
60/138,844	10 June 1999 (10.06.99)	US

(71) Applicant *(for all designated States except US)*: THOMSON LICENSING S.A. [FR/FR]; 46, quai Alphonse Le Gallo, F–92648 Boulogne Cedex (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: ESKICIOGLU, Ahmet, Mursit [TR/US]; 8235 Lakeshore Trail, Apt. #125, Indianapolis, IN 46250–4607 (US). VIRAG, David, Emery [US/US]; 7485 Cherry Hill Drive, Indianapolis, IN 46254–9769 (US). DUFFIELD, David, Jay [US/US]; 5459 Fall Creek Road, Indianapolis, IN 46220 (US). DEISS, Michael, Scott [US/US]; 1103 Indian Pipe Lane, Zionsville, IN 46077 (US). BEYERS, Billy, Wesley, Jr. [US/US]; 1075 Arrow Wood Drive, Carmel, IN 46033–9046 (US).

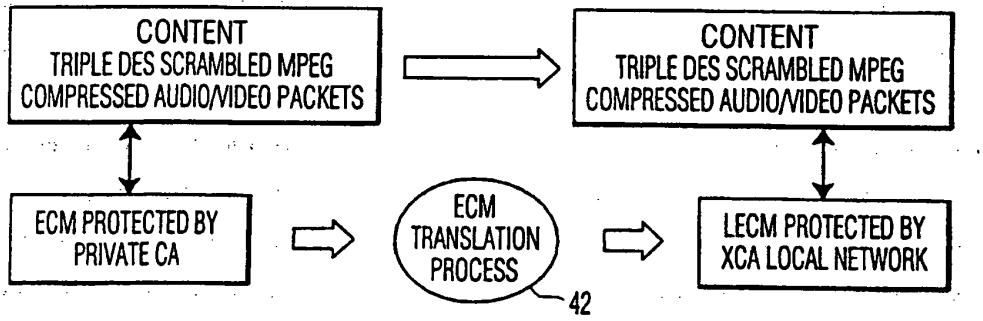
(74) Agents: TRIPOLI, Joseph, S. et al.; Thomson Multimedia Licensing Inc., P.O. Box 5312, 2 Independence Way, Princeton, NJ 08540 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(54) Title: A GLOBAL COPY PROTECTION SYSTEM FOR DIGITAL HOME NETWORKS



(57) Abstract

A method for providing local security of audio and video content during transmission and storage within digital home networks. Scrambled content may be recorded in all conditions, however, only authorized copies are processed for descrambling and viewing. Content is protected within a network by rebundling the keys required for descrambling, e.g., the TDES keys, into a new ECM (LECM), which is protected by a local public key.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

IPR2025-00305
ASUS EX1002 Page 228

A GLOBAL COPY PROTECTION SYSTEM FOR DIGITAL HOME NETWORKS

Field of the Invention

This invention provides local security of audio and video content during transmission and storage within digital home networks. Scrambled content may be recorded in all conditions, however, only authorized copies are processed for descrambling and viewing.

Background of the Invention

Copyright owners and content creators, such as movie studios and production companies, have a need for protecting their investment, for example, movies, programming, services, software, or the like. Such content has typically found its way to the consumer through network broadcasts, premium programming cable or satellite channels, pay-per-view events, and retail sales and rentals of videocassettes.

Analog videocassette recorders (VCRs) allow consumers to view content at their convenience. Fortunately, such analog VCRs produce a reduction in quality of each generational recording that the second or third generation is usually unacceptable to most viewers. However, with digital technology, the intrinsic generational degradation characteristic of the analog technology no longer exists. The nature of digital storage and transmission allows endless generations of copies to be produced with the same quality as the original master. Today, most products that receive digital video services have only analog outputs. Future products with digital outputs will allow for the convenience of networked systems and higher quality recording. A home network, which receives content for display and storage, must now also protect content against illegal copying or distribution.

The Draft Video Home Recording Act of 1996 defines the Copy Generation Management System (CGMS) as a mechanism to manage the creation of copies, not the viewing of those copies. The rights of copyright owners do

not map nicely into the concept of CGMS. Indeed, copyright owners have a greater interest in controlling the actual viewing of material as opposed to the copying of the material. Today, even using industry standard analog copy protection techniques, the emphasis is placed on the individual ability to view the copy. This is different from constraining the copying device from actually creating that copy.

These issues are exasperated due to the dramatic developments in digital media distribution such as the Internet. Therefore, there is a need to provide a secure solution for protecting the intellectual property of the copyright owners.

Summary of the Invention

The present invention resides, in part, in recognition of the described problem and, in part, in providing a solution to above problems. Generally, the present invention provides a method for managing access to a scrambled program content. The invention protects content within a network by rebundling the keys required for descrambling, e.g., the TDES keys, into a new ECM (known as an LECM). This method may comprise receiving a scrambled program (e.g., a scrambled data component and a descrambling key) in the first device, and rebundling the descrambling key using a unique key associated with the first device. The descrambling key is obtained from the rebundled descrambling key in a second device and used for descrambling the scrambled data component.

In accordance with one aspect of the present invention, the descrambling key is encrypted and the step of rebundling comprises decrypting the encrypted descrambling key using a key associated with the scrambled program and re-encrypting the descrambling key using a key associated with the first device to produce the rebundled descrambling key (i.e., LECM).

In accordance with another aspect, the present invention provides a method for managing access, within a network, to a scrambled program received from a service provider. The encrypted descrambling key associated with the

scrambled program is decrypted in the access device using a key associated with the service provider and then the key is re-encrypted using a public key associated with said access device. The presentation device decrypts the re-encrypted descrambling key and descrambles the scrambled data component using the descrambling key. This invention may also be utilized for managing access to a scrambled pre-recorded program.

In accordance with yet another aspect, the present invention provides a method for recording a scrambled program received from a service provider. The method comprises receiving the scrambled program and decrypting the encrypted descrambling key in the access device, which in this case may be a video recording device, using a key associated with the service provider. The descrambling key is re-encrypted using a public key associated with the access device. The recording device records the scrambled data component and the re-encrypted descrambling key on media coupled to the recording device.

Brief Description of the Drawings

Figures 1a and 1b are system block diagrams of the XCA architecture in accordance with the present invention;

Figure 2 is a block diagram of a generic XCA device employed in the XCA architecture of Figure 1;

Figure 3 illustrates a model for distributing the public and private keys in accordance with the invention of Figure 1;

Figure 4 is a block diagram illustrating the generation of an LECM in accordance with the invention of Figure 1;

Figure 5 is a block diagram illustrating the flow of content in accordance with the invention of Figure 1;

Figure 6 is a schematic diagram illustrating the protection of the NRSS interface in accordance with the invention of Figure 1; and

Figures 7 and 8 are schematic diagrams for creating secure authenticated links in accordance with the invention of Figure 1.

Where applicable, the same element numbers were used throughout these figures.

Detailed Description of the Drawings

A global protection system for digital home networks, also known as extended conditional access, or XCA, is defined in this application. XCA is a replaceable copy protection system designed to be used with renewable security devices such as smart cards. The Consumer Electronics Manufacturers Association (CEMA) has established 3 standards for interconnecting a digital television with other devices; (1) EIA-775 - Digital Television 1394 Interface; (2) EIA-761 - 8-VSB Remodulator Interface; and (3) EIA-762 - 16 VSB Remodulator Interface. EIA-761 and EIA-762 are one-way transmission interfaces while EIA-775 supports bi-directional communications. Although XCA can be successfully employed with any of these interconnection standards, it is not limited to these three standards.

The flow of information is primarily one-way in an XCA system. Content flows from the source to the display maintaining its original scrambling. Because the content is chain protected instead of link protected, there is no need for consecutive links to negotiate or establish keys. All information flows strictly from the source device to the sink device, that is, always toward the presentation device (typically a digital television (DTV) or set-top box in combination with a television) for final viewing.

The following definitions are used to describe the present invention. Encryption or scrambling is the process of transforming plaintext into ciphertext (i.e., $E_{c,k}[M]$; the message M is encrypted with cipher algorithm C using key K); decryption or descrambling is the reverse process. Conventionally, encryption and decryption are used when discussing control words or keys, and scrambling and descrambling are used when discussing audio/video content. A control word (CW) is the key used to scramble and descramble audio/video content. A cryptosystem is a system for achieving confidentiality, an information security objective.

IPR2025-00305
ASUS EX1002 Page 232

In a symmetric cryptosystem, the encryption and decryption keys are the same or can easily be determined from each other. In an asymmetric or public key cryptosystem, the encryption and decryption keys differ in such a way that at least one key is computationally difficult to determine from the other. Although the two keys are mathematically related, it is not possible to derive the private key with reasonable computational resources. As described below in further detail, each access device contains a unique public key for the purposes of locally encrypting the descrambling keys (LECMs). This unique public key is either stored in the access device during manufacturing or sent from a conditional access (CA) server when the access device is initialized in the field. During initialization, as described below in further detail, the access device may contact the CA server to obtain the unique public key using the identification of the access device.

Particularly, XCA protects the digital MPEG-2, or equivalent, encoded audio/video (A/V) content during transmission and storage. This is accomplished by mapping the three basic controls, namely, "playback control", "record control" and "one-generational control" into "viewing control". With XCA, content of economic value is always scrambled, either under the control and responsibility of the distributor or within the confines of the consumer's home network. The recording of scrambled content is always permitted in all conditions, however, only authorized copies are processed for descrambling and viewing in licensed devices.

XCA addresses the two critical elements for viewing control: time and space. Viewing control over time provides a mechanism to regulate when content can be viewed today or in the future. Viewing control over space regulates where and who may view this material. Together, these domains span a complete viewing space giving the copyright owner full controls over how content should be distributed and used.

XCA provides for three levels of entitlements. First, content that is free to distribute in an unlimited fashion is "free-copy" content. Examples of "free-copy" content may be broadcast television, infomercials or similar material that is supported by advertisers. Local View Programming, or "copy-once" content, provides a single household the ability to create and view a copy regardless of time. However, such a copy cannot be transported to other local networks because an LECM generated in one network cannot be decrypted in another local network. Examples of this type of content may be sporting events or premium services. Finally, "never-copy" or Immediate View Programming content allows for only the real-time viewing, i.e., recorded copies will never be viewable. Examples of this type of content may be pay-per-view programming or other high-value content.

Figures 1a and 1b illustrate a distinct characteristic of the XCA architecture 10, that is, the notion of conditional access and local protection. Content of economic value 11 whether from a tape, DVD, cable, satellite or terrestrial broadcast is usually delivered via a private conditional access service. The audio/video content and keys are protected and supplied to all the subscribers of the service using a private conditional access architecture. Subscribers who purchase content are supplied with the necessary keys for descrambling the content. Access device 14, for example a set-top box, usually in conjunction with a smart card, obtains or generates the keys for descrambling the video content. In the XCA architecture, this is the process of conditional access. Local protection is the protection of the content within the boundaries of the home network, after the access device receives the scrambled program from the service provider.

In general, a consumer electronic (CE) device 20 ("XCA device") employed within XCA architecture 10 is defined in Figure 2. Such a device has, at a minimum, a switching unit 22 and a digital input 24. Depending on the device type, it may also contain one or more of the following elements; a security device 26 (typically renewable), storage unit 28, an analog output 30 and/or a

digital output 34. Certain device types are defined with specific functionality, for example, (1) XCA Access Device 14 (e.g., set-top box, DVD player, DTV) creates "XCA protected content", (2) XCA Presentation Device 16 (e.g., DTV) descrambles "XCA protected content", (3) XCA Recording Device 18 (e.g., DVHS or DVD recorder) only stores or plays but cannot create or descramble "XCA protected bit streams".

Access devices typically operate in combination with an XCA/NRSS Converter Card (see 26a of Figure 5). The XCA/NRSS converter card creates XCA protected content from private conditional access (CA) protected content or XCA globally protected content. Presentation devices, such as DTV 16, operate in combination with an XCA/NRSS Terminal Card (see 26b of Figure 5) for descrambling XCA protected content. If a DTV is used as an access device as well as a presentation device, the DTV may operate with both a converter card 26a and a terminal card 26b or the functionality of both may be integrated into one card.

The XCA architecture can handle (1) clear content that is not protected by any means, e.g., broadcast programs, (2) CA content that is scrambled by a CA system using ECMs to carry the control words (CWs), e.g., digital satellite or cable services, (3) XCA content that is scrambled by XCA using Local ECMs (LECMs) to carry the CWs or keys (the LECMs are encrypted using the public key associated with access device 16), and (4) NRSS content that is scrambled by the XCA NRSS copy protection scheme. In addition, XCA content that is scrambled using Universal ECMs (UECMs) to carry the CWs may also be processed by this system. UECMs are encrypted using one unique global public key common to all networks and may be used, for example, for pre-recorded content.

The typical functions of an XCA device of Figure 2 are described below. The digital input 24 comprises all the circuitry and software needed to acquire a digital signal. The digital input may be of the form of a digital bus (e.g., IEEE

1394), a telco, a LAN, RF VSB/QAM or the like. Similarly, the digital output 34 comprises all the circuitry and software needed to provide a digital signal and may be of the form of a digital bus (e.g., IEEE 1394), a telco, a LAN, RF VSB/QAM or the like.

Security device 26, whether renewable such as an NRSS card or embedded within a host device 20, handles CA functions and XCA functions and is able to transform the type of the content. Security device 26 may only be connected to a single XCA device at any one time and provides transformed content. The below table summarizes the permitted transformations.

Signal In \ Signal Out	Clear	CA	XCA	NRSS
Clear	Yes (T0)	No	No	No
CA	Yes (T4)	Yes (T0)	Yes (T1)	Yes (T2)
XCA	Yes (T5)	No	Yes (T0)	Yes (T3)
NRSS	No	No	No	Yes (T0)

The following transformations are applicable for both removable and embedded security devices:

T0 is the identity transformation, i.e., the output stream is exactly equal to the input stream. This allows card chaining.

T1 If the user has the right CA entitlements, then the security device recovers the CWs, and descrambles the content. It then generates the TDES keys, re-scrambles the content, and encrypts the LECMs using its public key. If the content source is an ATSC compatible system (i.e., TDES scrambling), descrambling may not be needed.

T2 If the user has the right CA entitlements, then the security device recovers the CWs, and descrambles the content. It then re-scrambles the content following the requirements of the XCA NRSS interface protection system, described below in further detail. The CA provider defines this transformation.

T3 If the user has the right XCA entitlements, then the security device descrambles the content using the CWs of the LECMs. It then re-scrambles the content following the requirements of the XCA NRSS interface protection system.

The following two transformations only apply to embedded security devices:

T4 If the user has the right CA entitlements, then the security device recovers the CWs, and descrambles the content. The CA provider defines this transformation.

T5 If the user has the right XCA entitlements, then the security device descrambles the content using the CWs of the LECMs.

A converter card supports at least transformation T1 and a terminal card supports at least transformation T3. In addition to the above requirements, if security device 26 is renewable and is capable of non-volatile storage of program content, then its storage shall not accept NRSS content. If security device 26 transforms content (e.g., scrambles/re-scrambles content or encrypts/reencrypts LECMs) then it shall conform to NRSS-A or NRSS-B. Finally, if security device 26 needs NRSS interface protection 35, then it shall use the XCA NRSS interface protection system, as referenced in EIA-679B (described below in further detail).

Storage unit 28 may either be fixed such as a hard drive or removable such as a recordable DVD, DVHS tape or the like. Storage unit 28 stores clear or XCA content and is able to replay the content later when requested by the system. That is, storage unit 28 is able to read, and optionally write, content; it does not transform the type of the content.

Presentation device 16, if necessary, descrambles 35 the NRSS copy protection stream and then decodes 36 the MPEG2 content . The descrambled

and decoded content is then presented to the user in an analog form by passing the content through digital-to-analog converter 38. The final outcome may be a physical signal such as a TV display or analog output of a hi-fi amplifier. Presentation device 16 may have one or more analog outputs, or uncompressed digital outputs. In these cases, the output is protected by the relevant copy protection system.

Switching unit 22 routes content within the XCA device. Its function is limited to routing only; it does not transform the type of the content. The following table defines the different routing options depending on content format.

Source \ Sink		Digital Output 34 or Storage Device 28	Security Device 26 (removable or embedded)	Presentation Device 16
Digital Input 24 or Storage Device 28	Clear	Yes	Yes	Yes
	Scrambled	Yes	Yes	NA[1]
	NRSS	No[2]	No[2]	No[2]
Security Device 26 (removable or embedded)	Clear	Yes	Yes	Yes
	Scrambled	Yes	Yes	NA[1]
	NRSS	No	Yes[3]	Yes

[1]Sending scrambled content to the presentation unit has no meaning. The presentation unit is incapable of descrambling the data, and thus cannot make any use of it.

[2]NRSS data should not be accepted by digital input or storage units. Thus it cannot be sent to other parts of the device.

[3]NRSS data can be passed from one security device to another only for the purposes of 'daisy chaining'. The content can be passed through subsequent devices in the chain, but the keys (or NRSS CP secrets) must not be disclosed to any other device (including security devices).

Before accepting a public key used for generating the LECM (i.e., rebundling of the ECM), an access device must be assured it is getting a public key that is legitimate, that is one generated by an authorized entity. Certification is one way of providing this assurance. Access devices shall only provide XCA content using a certified public key. A public key certificate is a signed message, which associates the public key with an originating entity.

A unique local public/private key pair is assigned to security device 26 employed in the XCA architecture. There are two types of security devices: devices with a converter module and devices with a terminal module. Every converter and terminal module may be assigned a unique 64-bit identification and a unique RSA public/private key pair of 1024-bit length.

The model for distributing the public and private keys for the converter modules is illustrated in Figure 3 wherein a Trusted Third Party (TTP), the CA provider itself or an independent organization, generates and keeps a copy of public/private keys in a database. The public key has to be in the converter module of the security device associated with the access device before any conversion takes place. The corresponding private key is downloaded to the terminal module when requested.

There are two modes for distributing public keys:

- Off-line mode: In this mode, a set of XCA_IDs is delivered to the card issuer or card manufacturer. Each ID is paired with the corresponding public key. The card issuer or the card manufacturer stores this information in the security device in a way to ensure its integrity.
- On-line mode: In this mode, only the XCA_IDs are delivered to the card issuer or card manufacturer. The XCA_ID is stored in the security device in a way to ensure its integrity. When first used in the field, the converter module requests its public key from the TTP. The transfer is made using the secure authenticated channel defined by the CA provider.

The TTP delivers the private key of a given converter module to a terminal module only in response to the request of this terminal module. The transfer shall use the secure authenticated channel defined by the CA provider. The terminal module shall ask for a private key of a given converter module when it receives a LECM from an unknown converter module. A converter module issues such a LECM at least at the beginning of each session. A session begins every time the access device delivers a content to a presentation device. The TTP has the responsibility to monitor the requests in order to detect malicious requests. The security policy associated with this task is determined by the CA provider as part of his risk analysis.

The communication between the converter/terminal modules 26a and 26b and the TTP will be under the control of the CA provider operating the XCA system. The TTP will select and implement appropriate communication channels and message protocols needed for key distribution. In implementing the XCA system, the CA provider may choose a particular communication channel or a private message protocol. The CA providers will need to collaborate and exchange data to ensure the interoperability of security devices in home networks. This need may arise if, for example, a converter card and a terminal are provided by different CA providers. When the terminal card requests the private key belonging to the converter card from the TTP, the TTP will have to obtain it from the CA provider that owns the converter card.

The keys for content descrambling are rebundled in LECMs by access device 14. That is, the encrypted ECMs, which carry the descrambling keys, are decrypted by access device 14 and then re-encrypted using a local public key associated with the access device to produce the LECM. Particularly, XCA system 10 achieves local security by only descrambling the content when it is to be viewed, for example, in conjunction with the local presentation device (e.g., digital television) 16. Private conditional access protects the transmission of the content from the service provider (i.e., tape, DVD or broadcast 11) to the user's

IPR2025-00305
ASUS EX1002 Page 240

access device 14. The XCA architecture protects the content in the local network.

Particularly, XCA operates on the philosophy that content should be encrypted at all times, including distribution and storage. Consider, for example, the delivery of premium programming from a multi-program video provider. Content is scrambled as it enters the home. The provider's private CA system is responsible for making available the content to the consumer according to the entitlements that have been agreed upon. In an ATSC-compliant digital delivery systems, the program is MPEG compressed and scrambled using the triple DES (TDES) algorithm. The keys for descrambling the program are contained in Entitlement Control Messages (ECMs) which themselves are encrypted in some private and unknown fashion. A consumer entitled to view the program must be handed either the descrambled transport stream or a scrambled transport stream with the keys necessary for descrambling when viewed. The first case does not provide for the protection of content.

As shown in Figure 4, XCA protects the content on the local network by rebundling (i.e., ECM translation) 42 the keys required for descrambling (i.e., the TDES keys) into a new ECM which is protected by a local public key associated with the access device (i.e., LECM). This process is typically performed in access device 14 and preferably in security device 26. In this fashion, the only device capable of recovering the TDES keys and hence descrambling the MPEG program is the local presentation device, e.g., DTV. Because every local network contains a unique set of public/private key pairs, only the local system which recorded or viewed the original content is capable of viewing any copies derived from its local network distributed content. Even if a rogue device making non-legitimate and unauthorized copies exists, they are viewable only within the local network.

The flow of content with the XCA domain is further explained using Figure 5. The CA and XCA functionality can be optionally removed from the access

device and placed in a special security device 26, known as a converter card 26a. Likewise, a terminal card 26b can optionally assume the CA, XCA and NRSS functionality (i.e., the security aspects) of presentation device 16. Particularly the flow of content within the XCA domain involves passing incoming CA content from access device 14 to CA module 44 of security device 26a. CA module 42 recovers the control words (CW) or keys for the CA content and passes the CWs to converter module 46 which generates the necessary LECM. Converter module 46 passes XCA protected content back to access device 14 which in turn passes the XCA protected content to presentation device 16. The XCA protected content is passed to security device 26b, particularly to terminal module 50 via CA Module 48. Terminal module 50 recovers the CW from the LECM and descrambles the XCA protected content. The clear content is now passed to NRSS CP module 52; both the NRSS CP module 52 and presentation device 16 participate to generate the scrambling key. The scrambling key is usually a symmetric key, but other approaches using a public key may be employed. The functionality of NRSS CP module 52 is shared by security device 26b (represented as 52a) and presentation device 16 (represented by 52b). NRSS CP module 52 scrambles, preferably using DES, the content using this scrambling key and then passes the scrambled content to NRSS CP module 52b in presentation device 36. NRSS CP module 52b descrambles the scrambled content for display.

In XCA systems, both real-time and pre-recorded content remains scrambled throughout the system. The XCA presentation device 16 using the copy protection system as defined by EIA-679 and EIA-796 accomplishes final descrambling. In this fashion, copy protection management is provided end-to-end, that is, from the source of scrambling to the final viewing display. As is illustrated in Figure 6, XCA protects the NRSS interface by rescrambling the content using single DES with keys generated randomly between the presentation device and the NRSS card. Known as the Diffie-Hellman key agreement, this protocol ensures a third party cannot recover the keys simply by tapping the smart card interface.

Particularly, the protection of the NRSS interface is based on three primary principles. Firstly, restricting the devices that may receive copy protected data by requiring a license. Secondly, scrambling data and protecting the keys so those passive devices cannot record signals and decode a clear bit stream. Finally, coupling the host presentation devices and terminal cards and authenticating the host devices so those active devices to record bit streams are difficult to create.

Therefore in general, the procedure for establishing an XCA protected NRSS link involves: (1) authenticating the presentation host device, (2) establishing a shared secret key that is unique to a particular presentation device/terminal card pair, (3) creating content protection keys (e.g., shared keys) in real time, (4) scrambling content returning to the host (e.g., DTV) with DES, and (5) descrambling content received by the host. These steps are illustrated in Figure 6.

Every XCA presentation device will be manufactured with a unique ID. This ID can be used to identify the manufacturer and a specific XCA presentation device. These ID's are warranted by the manufacturer to be unique, but are not certified or secure in any way. This allows a host to be uniquely identified for the purpose of security, yet makes device revocation virtually impossible to manage. Forging an apparently valid ID is very simple, but security methods outlined below eliminate any significant value in doing so.

NRSS based terminal cards can create a secure authenticated link with a presentation device by communicating with a trusted third party (TTP). Either the device ID or the model and serial number can be used to get the correct DH public key for a given host. In this scheme, as illustrated in Figure 7, the ID/serial number is sent to the TTP (steps 1 and 2). The TTP queries its manufacturers database for this host (step 3), determines the correct public key for this XCA Presentation Device (step 4), and sends some private authentication

to the CA module via a secure channel (step 5). Alternatively as illustrated in Figure 8, the card can request the public key from the host device (step 1) and send it to the CA head-end or TTP for authentication and storage (step 2). Many feasible communications messages and channels exist. Possibilities for communications channels are phone lines, return path communications, sending an EMM over a distribution network, or even shipping a physical unit.

The only devices allowed to use the XCA NRSS copy protection system outlined here are devices that do not have (1) a digital input that can receive data from the NRSS interface or (2) any means for mass storage that can receive data from the NRSS interface.

A shared secret shall be established between any given pair of a presentation device and a terminal card. At the terminal card's option, a single shared secret value can be used for all sessions, or, if additional security is desired, a new-shared secret can be created for each session. The procedure for secret creation is outlined in the copy protection framework for NRSS (EIA-679B part A section 20.3, or part B section 8.9.3). Control words for protecting content travelling across the NRSS interface shall be created according to the NRSS standard (EIA-679B part A section 20.5, or part B section 8.9.5).

The interval for updating NRSS content scrambling keys is the same as the interval for updating content scrambling keys in local network packets. The update rate in local network packets can be found using source_sequence_number in section. At each new source_sequence_number, a new NRSS key should be put into use. If the new key is the EVEN key in a negotiated pair, then a new negotiation should be started at the same time the new key is used. If this negotiation does not conclude before the next increment to source_sequence_number, then the terminal card should stop providing NRSS content because the host is not behaving properly. This requires that hosts (and cards) must be able to complete the key negotiation in less than 900mS.

3DOCID: <WO ____0056068A1_I_>

IPR2025-00305
ASUS EX1002 Page 244

Content being scrambled for protection over the NRSS interface shall conform to the NRSS standard (EIA-2679B part A sections 20.5.3 and 20.5.4, or part B sections 8.9.5.3 and 8.9.5.4). All packets in the main video stream and primary audio streams (that are actively in use) shall be scrambled.

XCA uses EIA-679A copy protection Format #1 with the below-defined field sizes.

datatype_id	id value	Size (bytes)
Host_id	05	8
N_host	07	8
N_module	08	8
Host DH Public Key	13	96
Module DH Public Key	14	96
CCI	18	8

All the CA systems that will be used in ATSC broadcast systems are assigned unique CA_system_IDs. Likewise, XCA uses a unique CA_system_ID to perform local conversion. The value chosen for XCA is 0x1180. The broadcasters shall include this ID in their list of CA providers. During the transmission of content, an unused PID shall be allocated for XCA LECMs. Each program that needs to be converted to XCA shall appear in a PMT, which includes the XCA_system_ID pointing to the allocated LECM PID. Empty packets with the LECM PID do not need to be inserted in the broadcast transport stream as the CA ECMs will be replaced by LECMs in the conversion process.

The MPEG2 transport stream consists of transport packets as shown below:

Syntax	No. of bits	Mnemonic
MPEG2_transport_stream() {		
do {		
transport_packet()		
} while (nextbits() == sync_byte)		
}		

Transport packets that are protected under XCA security are scrambled using Triple-DES, as per ATSC specifications on conditional access. The PIDs

carrying both non-local ECMs and local ECMs (LECMs) shall be specified by the Program Map Table defined in the MPEG2 standard.

The local ECM tables shall be packet aligned with the syntax defined below.

Syntax	No. of bits	Mnemonic
LECM_transport_packet(){		
sync_byte	8	bslbf
transport_error_indicator	1	bslbf
payload_unit_start_indicator	1	'1'
transport_priority	1	bslbf
PID	13	uimsbf
transport_scrambling_control	2	'00'
adaptation_field_control	2	'01'
continuity_counter	4	uimsbf
pointer_field	8	uimsbf
for (i=1; i<184; i++) {		
data_byte	8	uimsbf
{		
}		

wherein:

sync_byte — A fixed 8-bit field whose value is '0x47'.

transport_error_indicator — A 1-bit flag. When set to '1', it indicates that there is at least one uncorrectable bit error in the packet.

payload_unit_start_indicator — This 1-bit flag shall be set to '1', and the first byte of the payload of this transport stream packet shall carry a pointer_field.

transport_priority — A 1-bit flag. When set to '1', it indicates that the packet is of greater priority than the other packets having the same PID which do not have the bit set to '1'.

PID — A 13-bit packet identifier.

transport_scrambling_control — This 2-bit field shall be set to '00', meaning that the packet is not scrambled at the transport level.

adaptation_field_control — This 2-bit field shall be set to '01', meaning that there is no adaptation field following the transport stream packet header.

continuity counter — A 4-bit field that increments with each transport stream packet with the same PID. It wraps around to 0 after it reaches its maximum value.

pointer_field — This 8-bit field contains the number of bytes, immediately following the pointer field until the first byte of the first section that is present in the payload of the transport stream packet. A value of 0x00 indicates that the section starts immediately after the pointer field.

data_byte — Contiguous 184 bytes of data from Local Entitlement Control Message sections or packet stuffing bytes after Local Entitlement Control Message sections. Packet stuffing bytes of value 0xFF may be found after the last byte of a section. In this case, all following bytes until the end of the packet shall also be stuffing bytes of value 0xFF.

The Local Entitlement Control Message may comprise one or more sections each of, which may be variable in length. The LECM may comprise at least the (1) the XCA device identification of the security device that generated the LECM, (2) copy control information which may be used to enforce viewing rights, and (3) the descrambling keys.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in the art and it is intended to include such alterations within the scope of the appended claims.

IPR2025-00305
ASUS EX1002 Page 247

Claims

1 Method for managing access, within a network comprising a first device interconnected to a second device, to a scrambled program comprising:

(a) receiving said scrambled program in said first device, said scrambled program comprising a scrambled data component and a descrambling key;

(b) rebundling, in said first device, said descrambling key using a unique key associated with said first device;

(c) receiving, in said second device, said scrambled data component and said rebundled descrambling key;

(d) obtaining in said second device said descrambling key from said rebundled descrambling key; and

(e) descrambling, in said second device, said scrambled data component using said descrambling key.

2. The method of Claim 1 wherein said descrambling key is encrypted and the step of rebundling comprises:

(a) decrypting said encrypted descrambling key using a key associated with said scrambled program; and

(b) re-encrypting said descrambling key using said unique key associated with said first device to produce said rebundled descrambling key.

3. The method of Claim 2 wherein said unique key associated with said first device is a public key, said public key being located in said first device and a corresponding private key being located in said second device.

4. The method of Claim 2 wherein the step of rebundling is performed within a first smart card coupled to said first device and the steps of decrypting and descrambling are performed within a second smart card coupled to said second device.

5. The method of Claim 1 further comprising the step of initializing said first device within said network.

6. The method of Claim 5 wherein the step of initializing comprises the step of receiving said public key from a conditional access provider, said step of receiving comprising authentication of said conditional access provider.

7. The method of Claim 5 wherein said public key is prestored in one of said smart card and said access device.

8. The method of Claim 1 wherein said descrambling key is one of encrypted using a private means if said scrambled program is received from pre-recorded media and protected by a private means if said scrambled program is received from a service provider.

9. Method for managing access to a scrambled program comprising:

(a) receiving, from a first device, said scrambled program comprising a scrambled data component and a rebundled descrambling key encrypted using a network key;

(b) decrypting, in said second device, said rebundled descrambling key to generate said descrambling key; and

(c) descrambling, in said second device, said scrambled data component using said descrambling key.

10. Method for managing access to a scrambled program received from a service provider within a network having an access device and a presentation device, said method comprising:

(a) receiving said scrambled program in an access device, said scrambled program comprising a scrambled data component and an encrypted descrambling key;

(b) decrypting, in said access device, said encrypted descrambling key using a key associated with said service provider;

(c) re-encrypting said descrambling key, in said access device, using a public key associated with said access device;

(d) receiving, in said presentation device, said scrambled data component and said re-encrypted descrambling key;

(e) decrypting, in said presentation device, said re-encrypted descrambling key to obtain said descrambling key; and

(f) descrambling, in said presentation device, said scrambled data component using said descrambling key.

11. The method of Claim 9 wherein said scrambled program is prerecorded on media and provided to said access device, said encrypted descrambling key being received from said prerecorded media.

12. Method for recording a scrambled program received from a service provider, said method comprising:

a. receiving said scrambled program in an access device, said scrambled program comprising a scrambled data component and an encrypted descrambling key;

b. decrypting, in said access device, said encrypted descrambling key using a key associated with said service provider;

c. re-encrypting said descrambling key, in said access device, using a public key associated with said access device;

d. receiving, in a recording device, said scrambled data component and said re-encrypted descrambling key; and

e. recording said scrambled data component and said re-encrypted descrambling key on media coupled to said recording device.

13. The method of Claim 12 wherein said scrambled program is prerecorded on media.

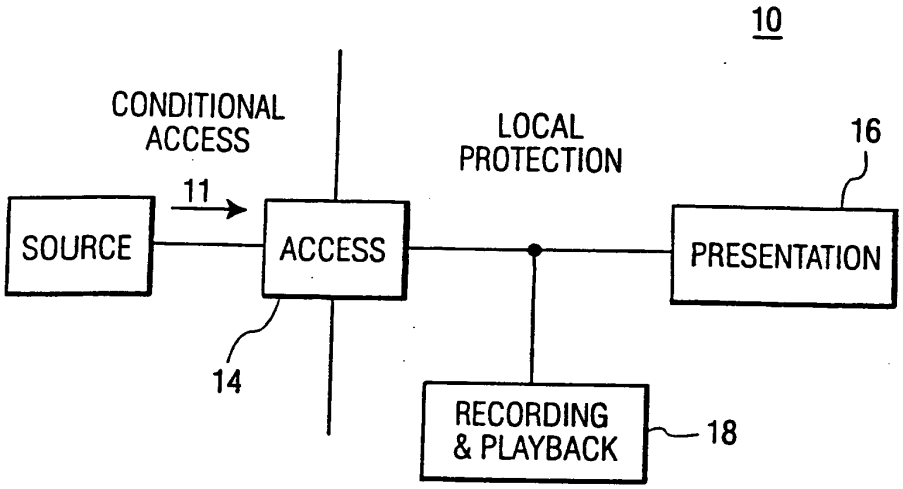

10
CONDITIONAL ACCESS
11
LOCAL PROTECTION
16
SOURCE
ACCESS
PRESENTATION
14
RECORDING & PLAYBACK
18

FIG. 1A

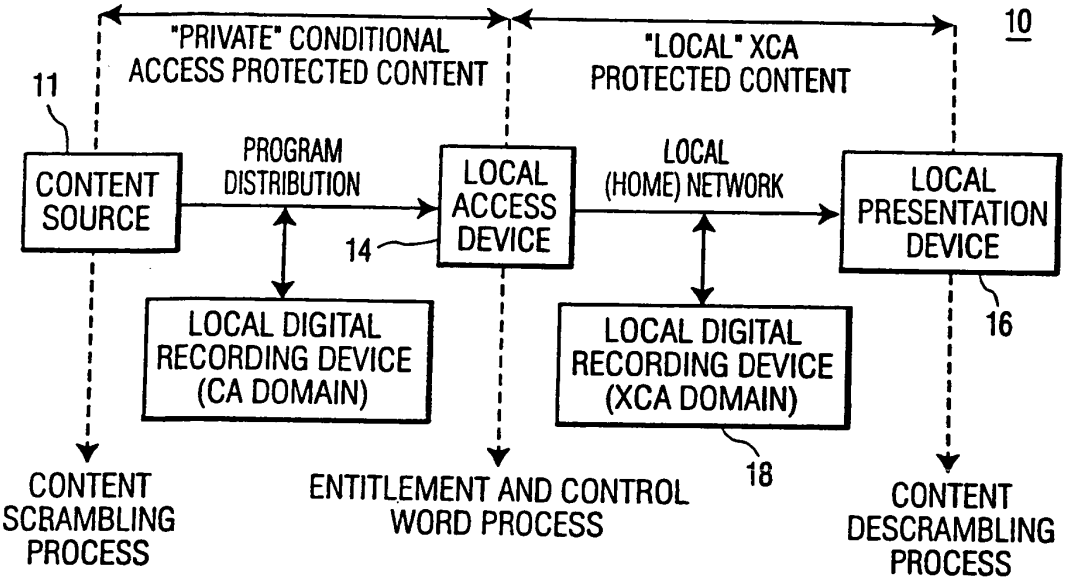
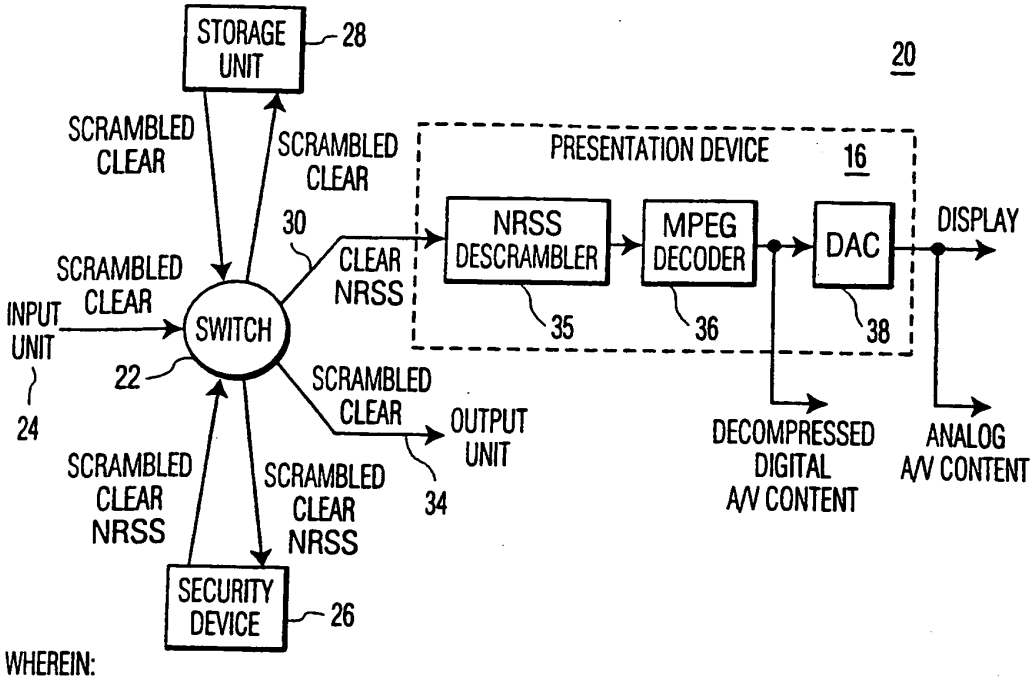

"PRIVATE" CONDITIONAL ACCESS PROTECTED CONTENT
"LOCAL" XCA PROTECTED CONTENT
10
11
CONTENT SOURCE
PROGRAM DISTRIBUTION
LOCAL ACCESS DEVICE
LOCAL (HOME) NETWORK
LOCAL PRESENTATION DEVICE
14
16
LOCAL DIGITAL RECORDING DEVICE (CA DOMAIN)
LOCAL DIGITAL RECORDING DEVICE (XCA DOMAIN)
18
CONTENT SCRAMBLING PROCESS
ENTITLEMENT AND CONTROL WORD PROCESS
CONTENT DESCRAMBLING PROCESS

FIG. 1B



WHEREIN:
TYPES OF CONTENT:

SCRAMBLED CA AND XCA CONTENT; CLEAR: UNSCRAMBLED MPEG TRANSPORT STREAM; NRSS: SINGLE DES SCRAMBLED TRANSPORT STREAM. THIS CONTENT IS INDISTINGUISHABLE FROM SCRAMBLED CONTENT WHEN THE DESCRAMBLING KEY(S) ARE NOT AVAILABLE.

FIG. 2

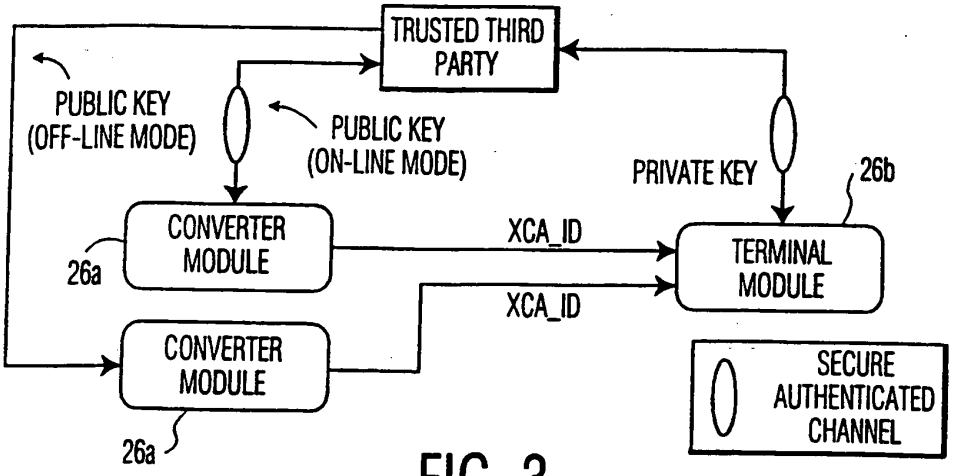


FIG. 3

SDOCID: <WO_____0056068A1_I_>

IPR2025-00305
ASUS EX1002 Page 253

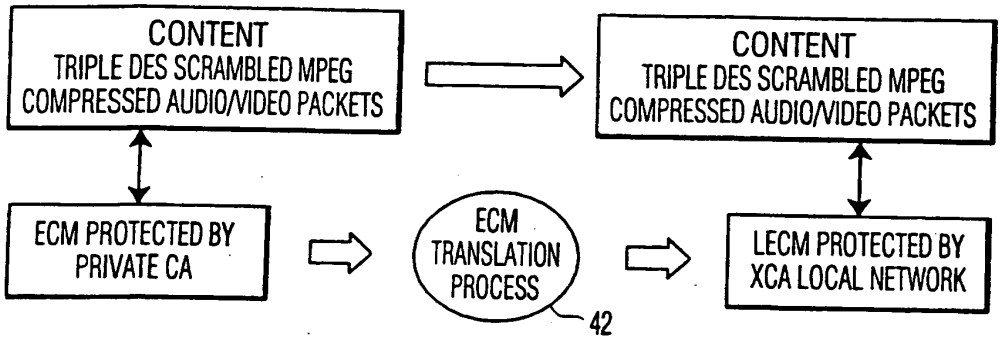

CONTENT
TRIPLE DES SCRAMBLED MPEG
COMPRESSED AUDIO/VIDEO PACKETS
CONTENT
TRIPLE DES SCRAMBLED MPEG
COMPRESSED AUDIO/VIDEO PACKETS
ECM PROTECTED BY
PRIVATE CA
ECM
TRANSLATION
PROCESS
42
LECM PROTECTED BY
XCA LOCAL NETWORK

FIG. 4

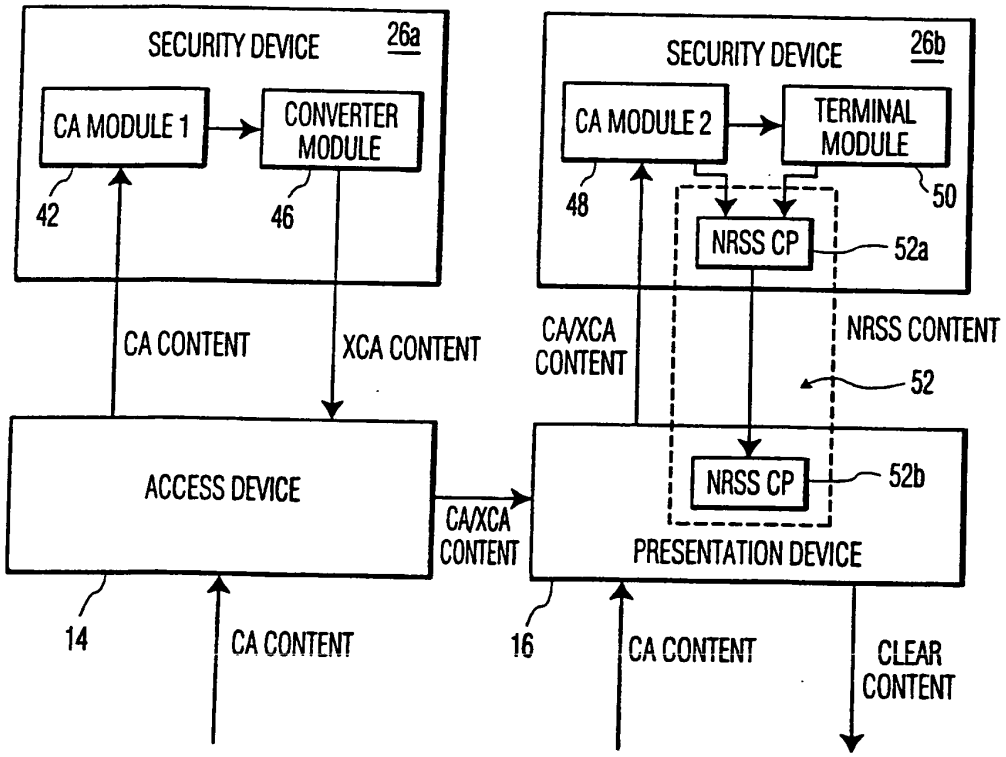

SECURITY DEVICE
26a
CA MODULE 1
CONVERTER
MODULE
42
46
SECURITY DEVICE
26b
CA MODULE 2
TERMINAL
MODULE
48
50
NRSS CP
52a
CA CONTENT
XCA CONTENT
CA/XCA
CONTENT
NRSS CONTENT
52
ACCESS DEVICE
NRSS CP
52b
CA/XCA
CONTENT
PRESENTATION DEVICE
14
CA CONTENT
16
CA CONTENT
CLEAR
CONTENT

FIG. 5

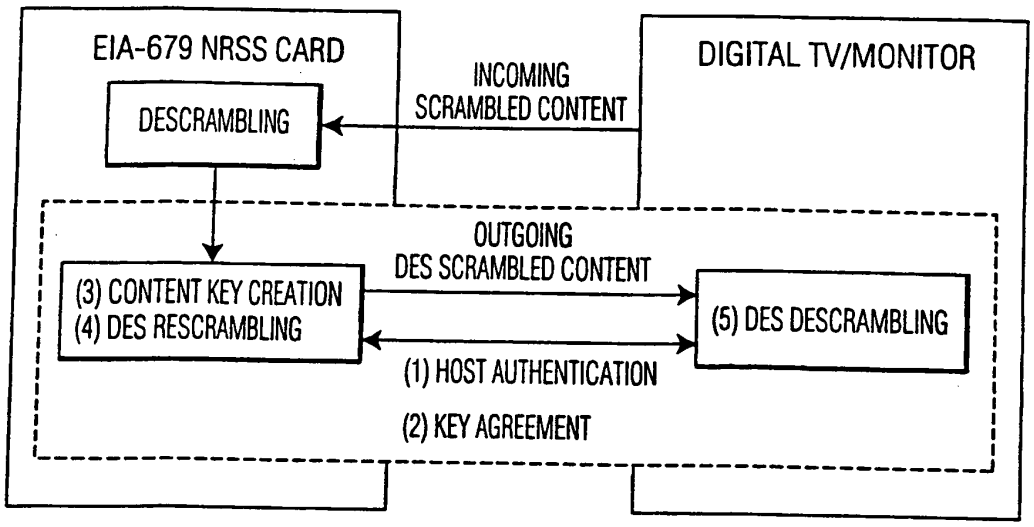


FIG. 6

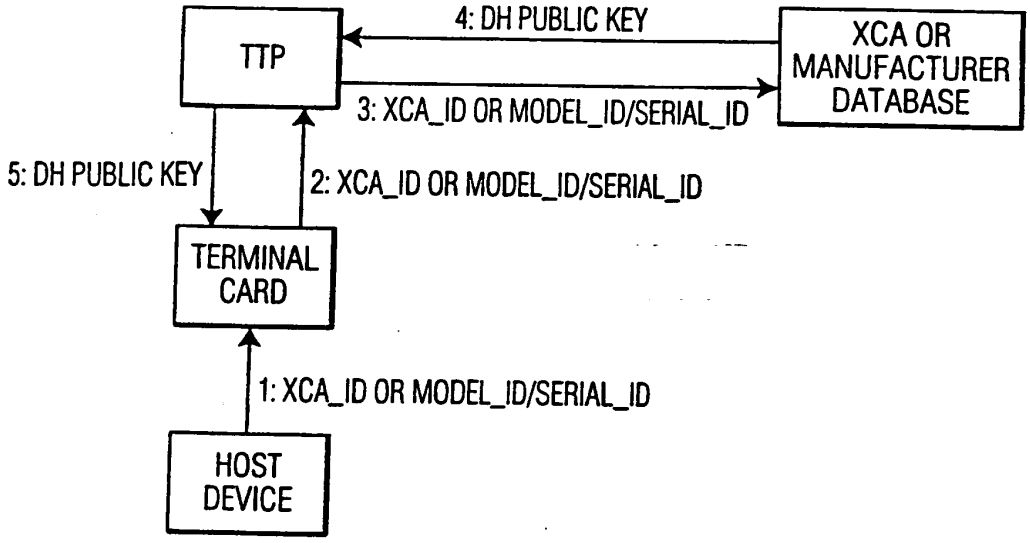


FIG. 7

SDOCID: <WO_____0056068A1_I_>

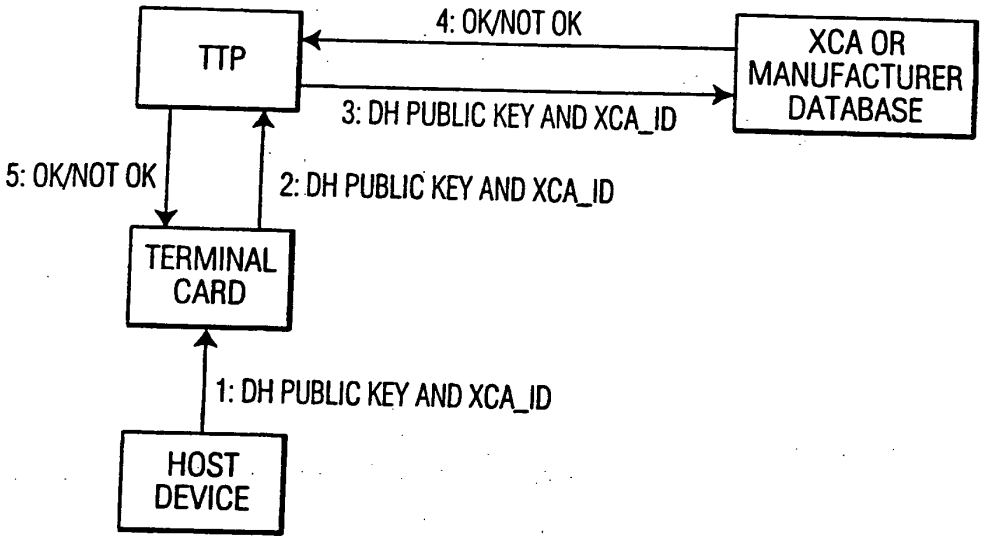


FIG. 8

DOCID: <WO_____0056068A1_I_>

IPR2025-00305
ASUS EX1002 Page 256

INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/US 00/06834

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N5/913 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 858 184 A (NDS LTD) 12 August 1998 (1998-08-12) page 5, column 6, line 9 -page 7, column 12, line 38 figures 1-5	1-3,5-13
A	EP 0 763 936 A (LG ELECTRONICS INC) 19 March 1997 (1997-03-19) page 4, column 6, line 25 -page 5, column 7, line 44 page 11, column 20, line 33 -page 14, column 25, line 15 figures 5-7,19-25	1-13

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2000	04/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van der Zaal, R

Form PCT/ISA/210 (second sheet) (July 1992)

DOCID: <WO 0056068A1 I >

IPR2025-00305
ASUS EX1002 Page 257

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern ıal Application No
PCT/US 00/06834

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0858184 A	12-08-1998	GB 2322030 A,B	12-08-1998
EP 0763936 A	19-03-1997	KR 166923 B	20-03-1999
		CN 1150738 A	28-05-1997
		JP 9093561 A	04-04-1997
		US 5799081 A	25-08-1998

Form PCT/ISA/210 (patent family annex) (July 1992)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 691 787 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
10.01.1996 Bulletin 1996/02

(51) Int Cl.[6]: **H04N 5/913**, H04N 7/167

(21) Application number: **95304743.8**

(22) Date of filing: **06.07.1995**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **08.07.1994 JP 180637/94**

(71) Applicant: **SONY CORPORATION**
Tokyo 141 (JP)

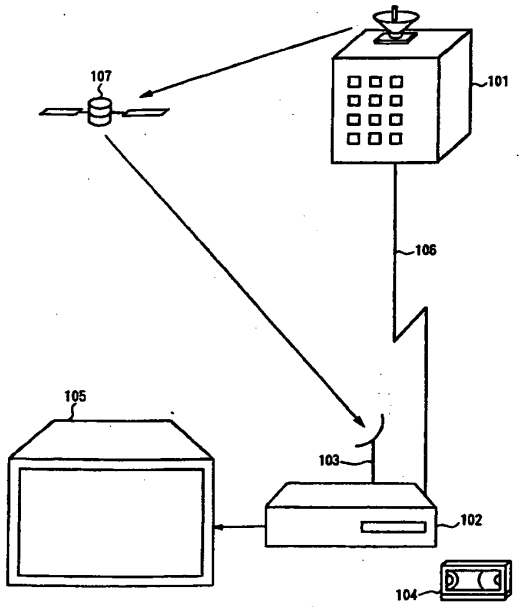
(72) Inventors:
- **Tsukamoto, Junichi, c/o Intellectual Prop. Div.**
  Tokyo 141 (JP)
- **Goto, Koichi, c/o Intellectual Prop. Div.**
  Tokyo 141 (JP)
- **Fukushima, Shinichi, c/o Intellectual Prop. Div.**
  Tokyo 141 (JP)

(74) Representative: **Pilch, Adam John Michael et al**
London EC4A 1DA (GB)

(54) Receiving controlled-access broadcast signals

(57) An apparatus and method for transferring from a broadcaster (101) to a receiver (102) a limited reproduction right in data. A signal indicating the limited reproduction right is transmitted by the broadcaster (101) and stored (104) by the receiver (102) with the data. The receiver (102) reproduces and processes the data as a function of this signal.

Fig. 1



EP 0 691 787 A1

Printed by Jouve (FR), 18, rue Saint-Denis, 75001 PARIS

Description

This invention relates to data communication in which controlled-access broadcast signals are received, such that, for example, a limited reproduction right in video data is transferred between a broadcaster and a receiver.

Commonly, video programming is transmitted from a broadcaster to a user via a satellite or cable communications system. In some systems, users are able to request, and broadcasters provide, select video programming through the use of individually addressable decoding receivers. The user's decoder is activated upon receipt of the user's address which is transmitted along with the requested video programming.

The drawback of such systems is that the user is often able to record the requested video programming for later reproduction. This later reproduction occurs without any royalty payment to the broadcaster or other holder of copyrights in the video programming. Further, the recorded video programming can be disseminated by the user to others for additional reproductions without corresponding royalty payments.

In accordance with the present invention, an apparatus for receiving, recording, and reproducing data signals is provided. A receiver receives transmitted data signals along with an access-control signal, the latter serving to control subsequent processing of the received data signals. The processed data signals are recorded in a first storage medium, and the access-control signal is stored in a second storage medium. When the processed data signals subsequently are reproduced from the first storage medium the access-control signal is retrieved from the second storage medium, and is used to control the reprocessing of the reproduced data signals.

A preferred embodiment of the present invention provides a system for the transfer between a broadcaster and a user of a limited reproduction right in transmitted data.

The preferred embodiment enables a user to request from a broadcaster a particular limited reproduction right in a selected video program, while preventing the reproduction of transmitted data by the user without adequate payment for each reproduction.

Other aspects of the present invention are set out in claims 1, 17, 23, 27, 36, 39 and 40.

The invention will now be described by way of example with reference to the accompanying drawings, throughout which like parts are referred to by like references, and in which:

Fig. 1 is a schematic diagram of a satellite broadcast system in which the present invention finds ready application;

Fig. 2 is a block diagram of a controlled-access broadcast digital video signal receiving system according to one embodiment of the present invention;

Fig. 3 is a block diagram of a controlled-access broadcast digital video signal receiving system according to another embodiment of the present invention;

Fig. 4 is a block diagram of a controlled-access broadcast digital video signal receiving system according to a further embodiment of the present invention;

Fig. 5 is a block diagram of a controlled-access broadcast digital video signal receiving system according to yet another embodiment of the present invention;

Fig. 6 is a flow diagram illustrating a communication and processing operation controlled by the controller of the controlled-access broadcast digital video signal receiving system of Fig. 2; and

Fig. 7 is another flow diagram illustrating another processing operation controlled by the controller of the controlled-access broadcast digital video signal receiving system of Fig. 2.

Figure 1 illustrates a satellite broadcast system incorporating a controlled-access broadcast signal receiving system 102 embodying the present invention. As explained in the following, it is preferred that the controlled-access broadcast signal receiving system 102 be specifically adapted to receive and process digital video data. Nevertheless, it should be appreciated that this system can be modified to accommodate other digital or analog signals. As it is understood that the system can easily be implemented to accommodate other types of data, the following explanation is specifically directed towards a controlled-access broadcast digital video signal receiving system 102.

The satellite television broadcasting system comprises a broadcasting station 101, the controlled-access broadcast digital video signal receiving system 102, an antenna 103, a video display 105, a communication link 106, and a satellite 107. The broadcasting station 101 broadcasts video signals and access-control signals to the controlled-access broadcast digital video signal receiving system 102 which processes the video signals as a function of the access-control signals.

The broadcasting station 101 transmits video and access-control signals to the receiving system 102 via the communication link 106, the satellite 107, or both. The communication link 106 is a signal transmission medium that couples broadcasting station 101 and receiving system 102. Preferably, communication link 106 comprises a conventional telephone line. Alternatively, communication link 106 includes any of a number of other transmission media, such as a land-based broadcast

system, a cable television system, a fiber optic network or the like.

Satellite 107 is a satellite broadcast signal relay station that receives signals from broadcasting station 101 and relays the signals to antenna 103. Antenna 103 receives signals from satellite 107 and supplies the signals to receiving system 102. Alternatively, satellite 107 can be replaced by any of a number of other transmission media, such as a land-based broadcast system, a cable television system, a fiber optic network or the like.

Receiving system 102 receives video signals and access-control signals supplied by broadcasting station 101 and processes (e.g. descrambles, decodes, and records) the signals. Typically, video signals are recorded on a storage medium and subsequently reproduced for display. Alternatively, video signals are recorded on a storage medium and processed for display to a user substantially simultaneously. Access-control signals are stored in a memory or, alternatively, recorded on a storage medium which may be the same storage medium on which the video signals are recorded. In a preferred embodiment, receiving system 102 is adapted to receive a storage cassette 104 containing a tape on which video and access-control signals are recorded. Alternatively, storage cassette 104 comprises a tape for storing video signals and a separate memory, such as a memory chip included therein, for storing access-control signals. In other embodiments, receiving system 102 is adapted to receive any of a number of other storage media, such as a video disc, a magnetic media diskette, a compact disc or the like. Video display 105, which preferably is a conventional display device, is coupled to and receives video signals from receiving system 102 for display to a user.

In a preferred recording mode of operation, broadcasting station 101 transmits video signals to satellite 107 which relays the signals to antenna 103 from which the video signals are coupled to receiving system 102. Also, broadcasting station 101 transmits access-control signals through communication link 106 to the receiving system. Receiving system 102 processes and records the video signals as a function of the access-control signals.

In a preferred reproduction mode of operation, the receiving system retrieves the previously stored access-control signals and uses those access-control signals to control the reproduction and processing of the previously recorded video signals. The video signals are supplied to video display 105 or to another peripheral device (not shown).

An alternate satellite television broadcasting system according to the present invention comprises each of the elements described above except that only one of communication link 106 and satellite 107 is included. The alternate system is otherwise interconnected as in the above-described embodiment. Through the single transmission medium, broadcasting station 101 transmits both video signals and access-control signals to receiving system 102.

In another variation, receiving system 102 transmits program requests, payment information, or other signals to broadcasting station 101 through one of the transmission media. Typically, communication link 106 is used for this purpose.

A first embodiment of the controlled-access broadcast digital video signal receiving system 102 according to the present invention is illustrated in Fig. 2 as system 102A. Receiving system 102A, is adapted for receiving, descrambling, enciphering, recording, deciphering and decoding digital video signals; and is comprised of a tuner 20, a descrambler 21A, an encipherer 22, a recording/reproducing section 23A, a decipherer 25, a decoder 26, an access controller 28A, a user interface 30, and a modem 31.

Tuner 20 receives input digital video signals, selects particular digital video signals, and supplies the selected signals to descrambler 21A. Preferably, input digital video signals are satellite broadcast digital video signals acquired by satellite antenna 103 which is coupled to tuner 20. Alternatively, input digital video signals are acquired from another transmission medium that is coupled to tuner 20. Preferably, a user controls tuner 20 to select signals from among different input digital video signals. The selected video signals include a time reference signal and a date reference signal.

Descrambler 21A is coupled to tuner 20 and descrambles scrambled digital video signals supplied therefrom. As is well known in the art, transmitted video signals are commonly scrambled or coded by a signal provider to prevent unauthorized reception of the video signals. Descrambler 21A supplies an unscrambled version of the digital video signals to encipherer 22. Further, descrambler 21A is coupled to a clock 27 to supply the received time reference signal and the date reference signal thereto.

Encipherer 22 is coupled to descrambler 21A, recording/reproducing section 23A, and access controller 28A. When enabled by the access controller, encipherer 22 encrypts, according to an encryption key, descrambled video signals supplied by descrambler 21A to produce encrypted video signals. The encrypted video signals are supplied to recording/reproducing section 23A for recording. However, the encrypted video signals cannot be displayed by ordinary means. It is contemplated that the encryption key is prestored in encipherer 22, or is supplied by access controller 28A, or is included in the video signals or in the access-control signals supplied by broadcasting station 101. When disabled by access controller 28A, encipherer 22 passes descrambled video signals from descrambler 21A directly to section 23A without encryption.

Recording/reproducing section 23A, through a record/playback head 24, or the like, records on storage medium 40 video signals supplied by encipherer 22. Section 23A, through head 24, also reads previously recorded video signals from storage medium 40 and sup-

ISDOCID: <EP 0691787A1 I >

EX1002 - Page 261
IPR2025-00305
ASUS EX1002 Page 261

plies the reproduced video signals to decipherer 25. Preferably, section 23A is a digital video tape recording/reproducing device (VTR) and storage medium 40 is a video tape. However, other types of storage media are contemplated, such as optical, magnetic or magneto-optic disc, solid-state memory, or the like.

Decipherer 25 is coupled to decoder 26 and, when enabled by access controller 28A, is adapted to decrypt, according to an encryption key, encrypted signals supplied by recording/reproducing section 23A. It is contemplated that the encryption key is prestored in decipherer 25, or is supplied thereto by access controller 28A, or is included in the video signals or the access-control signals supplied by broadcasting station 101, or is stored in storage medium 40, or is stored in access condition memory 29. When disabled, decipherer 25 passes video signals from recording/reproducing section 23A directly to decoder 26 without decryption.

As is well known in the art, video signals are commonly compressed or otherwise coded to facilitate their transmission through a transmission medium. Decoder 26 decodes such coded digital video signals as reproduced from storage medium 40 to produce uncoded digital video signals which are coupled to video display 105 for display. It is preferred that decoder 26 is adapted to decode digital video signals encoded in accordance with the Moving Picture Image Coding Experts Group (MPEG) standard.

Clock 27 is comprised of a clock device and a date device for tracking the time of day and the calendar date, respectively, known to those of ordinary skill in the art. Clock 27 is coupled to access controller 28A and supplies time signals and date signals thereto. The clock receives a time reference signal and a date reference signal from descrambler 21A and synchronizes its operation therewith.

User interface 30 is coupled to access controller 28A and supplies user input signals thereto. The user input signals are generated as a function of input supplied by a user to the user interface which may include a keyboard or user-operated switches. Typical user input signals include a command to display video signals, a command to record broadcast video signals, an authorization code, a request for a specific video program, and so on.

Modem 31 is coupled to access controller 28A and to communication link 106 and facilitates the communication of signals through the communication link between broadcasting station 101 (shown in Fig. 1) and the access controller. As communication link 106 is preferably a telephone line, modem 31 is preferably a conventional telephone line modem.

Access controller 28A is further coupled to an access condition memory 29. It will be appreciated that, as a function of the signals supplied to access controller 28A by clock 27, user interface 30, modem 31, and access condition memory 29, the access controller controls the operation of encipherer 22 and decipherer 25. As will be discussed in greater detail below, depending upon whether applicable conditions have been fulfilled, the access controller enables or disables the operation of encipherer 22 and decipherer 25. Access controller 28A stores access-control signals in and retrieves access-control signals from access condition memory 29. In an alternate embodiment, it is contemplated that the access controller 28A stores both access-control signals and the encryption keys of encipherer 22 and decipherer 25 in access condition memory 29.

Access-control signals indicate the conditions, if any, to be placed on the reproduction of the video component of the selected digital video signals. These conditions describe the circumstances under which a user may or may not reproduce the selected video signals. As a function of the access-control signals, the selected video signals recovered by descrambler 21A are processed prior to recording and processed again following reproduction. Depending on the particular conditions and circumstances, a user can be prevented entirely from accessing the selected digital video signals, given limited access to the signals, or given full access to the signals. Such conditions may include, but are not limited to, one or more of the following: (1) previous receipt of a payment signal from broadcasting station 101, (2) a numerical limit on the number of times particular video signals may be reproduced or displayed, (3) a temporal limit on the reproduction or display of video signals, and (4) previous receipt of a user authorization code. Preferably, the access-control signals are comprised of simple default values.

Also illustrated in Fig. 2 is storage cassette 104A which comprises access condition memory 29 and storage medium 40. Storage cassette 104A is, as a whole, removably connected to receiving system 102A. Access condition memory 29 stores access-control signals indicating the conditions, if any, to be placed on the reproduction and/or recording of video signals on storage medium 40. Preferably, access condition memory 29 is an integrated circuit RAM, integrated into storage cassette 104A but independent of storage medium 40, as has been proposed heretofore, and electrically connectable to access controller 28A. Storage medium 40 stores signals recorded thereon by head 24 and is preferably removably engaged therewith.

Operation of the embodiment of the controlled-access broadcast digital video signal receiving system 102A shown in Fig. 2 will be described below. An important feature of this embodiment is that access-control signals, corresponding to video signals that are to be recorded on or reproduced from storage medium 40, are stored in access condition memory 29. Access controller 28A controls the operation of encipherer 22 and decipherer 25 as a function of one or more of the access-control signals stored in access condition memory 29 and/or received from modem 31. In this manner, the encryption and decryption of video signals is controlled to prevent unauthorized reproduction of the video signals.

The configuration of the present invention is com-

EX1002 - Page 262
IPR2025-00305
ASUS EX1002 Page 262

patible with many different sequences of signal transfer between broadcasting station 101 and receiving system 102A. Examples of useful signal transfer sequences, implemented in different modes of operation of the present invention, will be described in detail below. Through the different modes of operation, video programs are securely transferred between a broadcaster and a consumer for recording, but the consumer's ability to display the programs can be subjected to limitations.

In a first video-on-demand mode, a user enters into user interface 30 a request for a specific video program. User interface 30 transmits this request to access controller 28A, which, in turn, communicates the user's request through modem 31 and communication link 106 to broadcasting station 101. The broadcasting station transmits the requested video program to satellite 107 which relays the video program to antenna 103 and supplies the video signals representing this program to tuner 20. It is expected that several video signals are coupled to tuner 20, which selects the particular video signals comprising the requested video program and supplies these selected video signals to descrambler 21A. The descrambler descrambles these broadcast video signals and supplies a descrambled version of the video signals to encipherer 22. Descrambler 21A also supplies a time reference signal and a date reference signal, which accompany the video program transmission, to clock 27.

Additionally, broadcasting station 101 communicates access-control signals through communication link 106 and modem 31 to access controller 28A for storage in access condition memory 29. The access-control signals serve to define the conditions or limitations, if any, upon the usage of the requested video program. In general, a user can either purchase or rent a particular video program from a broadcaster. In a prepayment method of purchase, a user pays for a video program and subsequently requests that the broadcaster transmit the program to the user's video receiving system. Broadcasting station 101 transmits the requested program and an access-control signal indicating that the video program can be unconditionally recorded and reproduced (FULL ACCESS). Access controller 28A stores the FULL ACCESS signal in access condition memory 29 to disable encipherer 22. Hence, descrambled video signals of the video program are supplied by descrambler 21A through encipherer 22, without encryption, to recording/reproducing section 23A, whereat the descrambled and unencrypted video signals are recorded on storage medium 40.

In a postpayment method of purchase, wherein a user elects to pay for a video program after it has been received by the user's receiving system, broadcasting station 101 transmits the particular video program to receiving system 102A along with an access-control signal indicating that the video program cannot be reproduced (NO REPRO). Access controller 28A stores the NO REPRO signal in access condition memory 29 and enables encipherer 22, causing it to encrypt, according to an encryption key, descrambled video signals of the video program supplied by descrambler 21A. Encipherer 22 supplies encrypted video signals to recording/reproducing section 23A, whereat the encrypted video signals are recorded on storage medium 40.

It is contemplated that the user subsequently purchases the video program from the broadcaster. Upon payment, broadcasting station 101 transmits an access-control signal to access controller 28A indicating that the recorded video program can be reproduced (REPRO OK), and this REPRO OK signal replaces the previously stored NO REPRO signal in memory 29. When the encrypted video signals subsequently are played back from storage medium 40, they are supplied to decipherer 25 which is enabled by the stored REPRO OK signal to decrypt the reproduced video signals.

In a second prepayment method of purchase, similar to the postpayment method, the user pays for the selected program prior to its transmission, but broadcasting station 101 first transmits the selected program to receiving system 102A along with a NO REPRO signal. Access controller 28A causes encipherer 22 to encrypt the video signals of the video program and the encrypted signals are recorded on storage medium 40 while the NO REPRO signal is stored in access condition memory 29. Upon completion of the video program transmission, broadcasting station 101 transmits a REPRO OK signal; and access controller 28A replaces the stored NO REPRO signal with the REPRO OK signal. Thus, the video program is recorded in encrypted form but the user can reproduce and decrypt the program an unlimited number of times. This second prepayment method has the advantage of producing video recordings that can only be reproduced in devices having compatible decryption capabilities.

Alternatively, a user can purchase the right to reproduce a video program a certain number (N) of times. The user thus "rents" the video program for N reproductions. In one mode, the user enters a request into user interface 30 to rent a video program for N reproductions. User interface 30 transmits the request to access controller 28A which forwards the request through modem 31 and communication link 106 to broadcasting station 101. Broadcasting station 101 transmits the requested video program along with an access-control signal indicating that the video program can only be reproduced N times (REPRO N TIMES). The access controller receives the REPRO N TIMES signal and stores it in access condition memory 29. The video program is received by tuner 20 and supplied to descrambler 21A which descrambles the video program and supplies descrambled video signals to encipherer 22. The encipherer, which is enabled by the access controller, encrypts the descrambled video signals, and supplies encrypted signals to recording/reproducing section 23A for recording on storage medium 40.

In another rental mode, wherein a user desires to rent a particular video program for a certain period of

ISDOCID: <EP 0691787A1 I >

EX1002 - Page 263
IPR2025-00305
ASUS EX1002 Page 263

time, an access-control signal designating the period of time during which reproduction of the requested video program is authorized is supplied by the broadcasting system. For example, the user may request to rent a particular video program for a certain number of days (D). Receiving system 102A transmits this request via communication link 106 to broadcasting station 101. The broadcasting station calculates the date Y, as a function of D, on which the reproduction right should expire, and transmits the requested video program along with an access-control signal indicating that reproduction is allowed until date Y (REPRO UNTIL DATE Y). The access-control signal is received by receiving system 102A and stored in access condition memory 29. The access controller enables the operation of encipherer 22; and as described above, the requested video program is received, selected by tuner 20, descrambled, enciphered, and recorded in enciphered form. Subsequently, the encrypted video program is reproduced, deciphered (so long as the reproduction operation is performed prior to date Y) and displayed.

As another example, a user can request to rent a particular video program for a certain number of hours (H). Receiving system 102A transmits this request via communication link 106 to broadcasting station 101 which calculates the time T, as a function of H, when the reproduction right should expire, and transmits the requested video program along with an access-control signal indicating that reproduction is allowed until time T (REPRO UNTIL TIME T). The received access-control signal is stored in access condition memory 29; and the operation of encipherer 22 is enabled by access controller 28A. As described above, the requested video program is received, selected, descrambled, enciphered, and recorded in an enciphered form.

Of course, there are many different methods of expressing the terms of a rental. The preceding expressions are intended merely as examples to assist in explaining the present invention and not as limits thereon. Further examples of useful rental terms include: reproduction of a video program for a certain number of hours or of days, or for a period of time in the future.

Analogous to the prepayment and postpayment methods of purchase, each rental of a video program can be prepaid or postpaid by the user. When the rental is prepaid, broadcasting station 101 transmits the requested program and the access-control signal specifying the terms of the rental to receiving system 102A which processes the video program (i.e., selectively encrypts the video signals) and stores the access-control signal as described above.

In contrast, when the rental is postpaid, broadcasting station 101 transmits the requested program and a NO REPRO signal to receiving system 102A, which encrypts and records the video program and stores the NO REPRO signal as described above. Upon proper payment, broadcasting station 101 transmits the access-control signal specifying the terms of the rental to the receiving system which replaces the NO REPRO signal in access condition memory 29 with the newly-transmitted access-control signal.

In a further variation, a certain segment of the video program can be made available for reproduction by a user in a "preview" mode of operation. In this "preview" mode a user can view a selected portion of the requested video program and later decide whether or not to purchase or rent the entire video program. In an illustrative implementation of the preview mode, the access-control signal corresponding to the preview segment is a REPRO OK signal and the access-control signal corresponding to the entire video program is a NO REPRO signal.

In a second video-on-demand mode, a user requests video programming from a broadcaster to be transmitted at a later time, perhaps the following day. The video programming may be, for example, one or more video programs selected by the user or a number of video programs selected by the broadcaster. In the latter case, it is contemplated that the user initially selects a particular type of video programming or selects video programming provided by a particular video program supplier.

The request for "delayed" transmission of the video programming is entered by the user into user interface 30. User interface 30 transmits this request to access controller 28A which communicates the user's request through modem 31 and communication link 106 to broadcasting station 101.

Some period of time later, broadcasting station 101 transmits the requested video programming to satellite 107 which relays the video programming to antenna 103. Preferably, transmission of the video programming occurs during periods when broadcasters are "off-the-air" or during periods of low viewership of broadcast video signals. Antenna 103 receives the video programming and supplies the video signals to tuner 20 from which the particular video signals comprising the requested video programming are supplied to descrambler 21A which, in turn, supplies a descrambled version of the video signals to encipherer 22.

In this mode, broadcasting station 101 also transmits two access-control signals via communication link 106 and modem 31 to access controller 28A. One access-control signal indicates that the video programming is to be erased on a certain date Y (ERASE ON DATE Y) and the other access-control signal is the NO REPRO signal. Access controller 28A stores the ERASE ON DATE Y signal and the NO REPRO signal in access condition memory 29. Encipherer 22, when enabled, supplies encrypted video signals to recording/reproducing section 23A for recording on storage medium 40.

Subsequently, but prior to date Y, the user selects a video program from the requested video programming stored on storage medium 40 and pays the fee to rent the selected program for a particular rental term. Upon payment, broadcasting station 101 transmits the ac-

EX1002 - Page 264
IPR2025-00305
ASUS EX1002 Page 264

cess-control signal indicating the appropriate rental condition to access controller 28A which replaces the previously stored NO REPRO signal in memory 29. Hence, the ERASE ON DATE Y signal remains stored in access condition memory 29.

Illustrative video signal reproduction modes of operation of receiving system 102A now will be described. The process is initiated when a user enters a command into user interface 30 to reproduce a prestored video program recorded on storage cassette 104A. The user interface transmits the command to access controller 28A which retrieves the access-control signal stored in access condition memory 29 of the storage cassette. The operation of decipherer 25 is controlled as a function of the particular access-control signal(s) that is retrieved.

If, for example, the retrieved signal is a FULL ACCESS signal, then access controller 28A disables decipherer 25. Recording/reproducing section 23A recovers video signals from storage medium 40 and supplies the reproduced video signals to decipherer 25, which passes the video signals to decoder 26. As described above, the reproduced video signals are unencrypted; and decoder 26 decodes the video signals and supplies uncoded video signals to video display 105.

If the NO REPRO signal is retrieved from access condition memory 29, access controller 28A disables the operation of decipherer 25. However, unlike the FULL ACCESS signal case, the video signals stored on storage medium 40 are encrypted. Hence, recording/reproducing section 23A reproduces encrypted video signals which are supplied to decipherer 25 to be passed directly to decoder 26 without decryption. The decoder decodes the encrypted video signals to produce uncoded but encrypted video signals which are supplied to video display 105. As a result, the video display either cannot display the video signals at all or can only display a distorted version of the original video program.

As a further alternative, access controller 28A may retrieve a REPRO OK signal from access condition memory 29 to enable the operation of decipherer 25. Recording/reproducing section 23A reproduces the encrypted video signals stored on storage medium 40 and supplies the encrypted signals to enabled decipherer 25 which decrypts the video signals and supplies unencrypted video signals to decoder 26. The decoder decodes the video signals and supplies the resulting uncoded and decrypted video signals to video display 105 for display. Because the video signals are uncoded and decrypted, video display 105 displays the reproduced video program without distortion.

As yet another alternative, when access controller 28A retrieves a REPRO N TIMES signal from access condition memory 29, the access controller 28A determines whether the number N is greater than a predetermined threshold value (e.g. zero). If the number N is not greater than the threshold value, then access controller 28A disables operation of decipherer 25 and reproduction of the stored video signal proceeds as in the NO REPRO signal case. On the other hand, if the number N is greater than the threshold value, then access controller 28A enables decipherer 25 and reproduction of the stored video signal proceeds as in the REPRO OK signal case.

After the video signal is reproduced from storage medium 40, if the number N is greater than the threshold value, access controller 28A subtracts one from the value of N to produce a new value N and writes a new REPRO N TIMES signal, utilizing the new value N, into access condition memory 29 whereat the previously stored REPRO N TIMES signal is replaced by the new REPRO N TIMES signal. According to this procedure, the particular video signals stored in storage medium 40 to which the REPRO N TIMES signal corresponds are only reproduced the number of times represented by the number N. The value N stored in access condition memory 29 thus reflects the remaining number of permitted reproductions of the particular video signals. Since the access condition memory is provided in the same storage cassette 104A as storage medium 40, and the video signals are encrypted on the storage medium, the video signals can only be reproduced for display N times even if the cassette is loaded into another receiving system, at least until a new access-control signal is stored.

When, as described above, a video program is rented for only a certain period of time, access controller 28A retrieves the corresponding access-control signal from access condition memory 29 and also receives a clock signal and a date signal from clock 27. The clock signal and the date signal are compared to the retrieved access-control signal, and if the particular condition expressed in the access-control signal is satisfied such that reproduction is allowed, then decipherer 25 is enabled and reproduction of the stored video signals proceeds as in the REPRO OK case. However, if the condition expressed by the access-control signal is not satisfied such that reproduction of the video signals is not allowed, then the decipherer is disabled and reproduction of the stored video signals proceeds as described with respect to the NO REPRO signal.

For example, when access controller 28A retrieves a REPRO UNTIL DATE Y signal from access condition memory 29, it compares the date signal from clock 27 to the date Y. If the date from clock 27 is prior to date Y, then the access controller enables the operation of decipherer 25 to decrypt the reproduced, encrypted video signals. In a similar fashion, when the access controller retrieves a REPRO UNTIL TIME T signal from the access condition memory, it compares the time signal supplied by clock 27 with the time T. If the time indicated by the time signal is prior to time T, then reproduction of the stored video signals proceeds as described with respect to the REPRO OK signal.

In an analogous manner, when access controller 28A retrieves an ERASE ON DATE Y signal from access condition memory 29, it compares the date signal from clock 27 to the date Y. If the date indicated by clock 27

ISDOCID: <EP 0691787A1 I >

EX1002 - Page 265
IPR2025-00305
ASUS EX1002 Page 265

is the same as or past date Y, then the access controller controls recording/reproducing section 23A to erase the video signals stored on storage medium 40. A suitable control channel, or link, may be provided between access controller 28A and recording/reproducing section 23A.

An alternate embodiment of receiving system 102A additionally includes a connection between descrambler 21A and access controller 28A. Here, scrambled access-control signals that are transmitted by broadcasting station 101 along with the video signals are supplied to and descrambled by descrambler 21A from which they are coupled to the access controller. In this alternate embodiment, video signals are recorded and reproduced as described above, and encipherer 22 and decipherer 25 are selectively enabled and disabled in response to the received access-control signals in the same manner as has been discussed.

As will be appreciated by one of ordinary skill in the art, each of the abovedescribed modes of signal reproduction wherein the user has prepaid for the video programming can be achieved substantially simultaneously with the recording of the broadcast video signals. In such a mode of operation, recording/reproducing section 23A functions both to record the processed broadcast video signals and to supply the video signals to decipherer 25. Decipherer 25, controlled by access controller 28A, decrypts the video signals as a function of the access-control signal to be stored in access condition memory 29 and decoder 26 decodes the resulting video signals for immediate display on video display 105.

Another embodiment of the controlled-access broadcast digital video signal receiving system 102B according to the present invention is illustrated in Fig. 3. Receiving system 102B differs from aforedescribed receiving system 102A in that receiving system 102B stores access-control signals and video signals in the same storage medium 40 of storage cassette 104B.

Recording/reproducing section 23B, through head 24, records on storage medium 40 in storage cassette 104B video signals supplied by encipherer 22 and access-control signals supplied by access controller 28B; and also reads previously recorded video signals and previously recorded access-control signals from the storage medium. The reproduced video signals are supplied to decipherer 25 and the reproduced access-control signals are supplied from the recording/reproducing section to access controller 28B. As before, recording/reproducing section 23B is a digital video tape recording/reproducing device (VTR) and storage medium 40 is a video tape; although the storage medium may be a magnetic disc, an optical disc, a magneto-optic disc, a solid-state device, or other recordable medium. It is also preferred that the access-control signals be stored in one or more sub-code regions of the storage medium.

When enabled by access controller 28B, decipherer 25 decrypts, according to an encryption key, encrypted signals reproduced by recording/reproducing section 23B. It is contemplated that the encryption key is prestored in the decipherer or is supplied thereto by access controller 28B, or is included in the video signals or the access-control signals supplied by broadcasting station 101, or is stored in and read from storage medium 40. When disabled, decipherer 25 passes video signals from recording/reproducing section 23B directly to decoder 26 without decrypting such signals.

As a function of the signals supplied to access controller 28B by clock 27, user interface 30, modem 31, and recording/reproducing section 23B, the access controller controls the operation of encipherer 22 and decipherer 25 as has been described previously. Specifically, depending upon whether applicable conditions have been fulfilled, the access controller enables or disables the operation of encipherer 22 and decipherer 25.

Each signal transfer sequence, including variations thereon, described above with respect to receiving system 102A is also implemented in similar modes of operation of receiving system 102B. It will be appreciated, then, that the modes of operation of receiving system 102B are substantially identical to the modes of operation of receiving system 102A with the following illustrative exceptions. Access controller 28B functions in the same manner as access controller 28A, except that access-control signals are stored, through recording/reproducing section 23B, in storage medium 40, instead of in a separate access condition memory. Recording/reproducing section 23B functions in the same manner as section 23A except that section 23B additionally records access-control signals on and reproduces access-control signals from storage medium 40. The reproduced access-control signals are supplied from recording/reproducing section 23B to access controller 28B.

Similar to the alternate embodiment discussed in conjunction with Fig. 2, an alternate embodiment of receiving system 102B additionally includes a connection between descrambler 21A and access controller 28B so that scrambled access-control signals that are transmitted by broadcasting station 101 along with the video signals are descrambled and supplied to the access controller. Of course, access controller 28B uses these access-control signals in the same manner as discussed above.

A further embodiment of the controlled-access broadcast digital video signal receiving system 102C according to the present invention is illustrated in Fig. 4. Receiving system 102C, is adapted for receiving, descrambling, decoding, recording, and reproducing digital video signals and is similar to the aforedescribed receiving system 102A of Fig. 2. As in receiving system 102A, receiving system 102C stores access-control signals in access condition memory 29 of storage cassette 104A, while the video signals are stored on storage medium 40 of the storage cassette.

Fig. 4 differs from Fig. 2 in that descrambler 21C of receiving system 102C is coupled to access controller 28C, recording/reproducing section 23A, and decoder

EX1002 - Page 266
IPR2025-00305
ASUS EX1002 Page 266

26; and encipherer 22 and decipherer 25 are not provided as separate circuits. When enabled by access controller 28C, descrambler 21C descrambles video signals supplied by tuner 20 and supplies an unscrambled version of the digital video signals to recording/reproducing section 23A. Also, when enabled by the access controller, descrambler 21C descrambles video signals reproduced by recording/reproducing section 23A and supplies an unscrambled version of the digital video signals to decoder 26. When disabled by access controller 28C, descrambler 21C passes scrambled video signals from tuner 20 directly, without encryption, to section 23A and also passes video signals reproduced by the recording/reproducing section directly, without decryption, to decoder 26. Scrambled video signals can be recorded but they cannot be displayed in scrambled form.

It will be appreciated that access controller 28C functions in the same general manner as access controller 28A, except that descrambler 21C is controlled in accordance with the access-control signals rather than encipherer 22 and decipherer 25.

At those aforedescribed operational steps where access controller 28A enables encipherer 22, access controller 28C disables descrambler 21C to pass scrambled signals to the recording/reproducing section; and where access controller 28A disables encipherer 22, access controller 28C enables descrambler 21C to supply descrambled signals to the recording/reproducing section. However, in the operational steps where access controller 28A enables decipherer 25, access controller 28C similarly enables descrambler 21C to descramble the signals reproduced by the recording/reproducing section. Where access controller 28A disables decipherer 25, access controller 28C similarly disables descrambler 21C to pass to decoder 26 signals reproduced by the recording/reproducing section.

In an alternate embodiment of receiving system 102C, access-control signals, transmitted by broadcasting station 101 along with video signals, are received through antenna 103 and supplied by tuner 20 to descrambler 21C for descrambling and for coupling to access controller 28C.

A still further embodiment of the controlled-access broadcast digital video signal receiving system 102D according to the present invention is illustrated in Fig. 5. Receiving system 102D is seen to be a combination of portions of receiving system 102C and receiving system 102B (Fig. 3). Similar to receiving system 102B, receiving system 102D stores access-control signals and video signals in the same storage medium 40 of storage cassette 104B. Recording/reproducing section 23B supplies the reproduced video signals to descrambler 21C and supplies the reproduced access-control signals to access controller 28D.

It will be appreciated that the modes of operation of receiving system 102D are substantially similar to the modes of operation of receiving system 102C with the following illustrative exceptions. Access controller 28D functions in the same manner as access controller 28C, except that access-control signals are stored in storage medium 40 instead of in a separate access condition memory. Recording/reproducing section 23B functions in the same manner as section 23A except that section 23B additionally records access-control signals on and reproduces access-control signals from storage medium 40. The reproduced access-control signals are supplied from recording/reproducing section 23B to access controller 28D.

Similar to the alternate embodiment discussed in conjunction with Fig. 4, access-control signals, transmitted by broadcasting station 101 along with video signals, are received through antenna 103 and supplied by tuner 20 to descrambler 21C for descrambling; and the descrambled access-control signals are supplied to access controller 28D. It is seen that access controller 28D receives access-control signals from recording/reproducing section 23B and either from modem 31 or from descrambler 21C, or from both.

Fig. 6 is a flow diagram of a preferred mode of operation of receiving system 102A of Fig. 2, as controlled by access controller 28A, wherein a user orders from a broadcaster a limited or an unlimited right (as may be desired) to reproduce a video program. The user initiates the process by entering a request for a particular video program at user interface 30. The process begins at step S60, where access controller 28A causes modem 31 to connect to broadcasting station 101.

Access controller 28A transmits identification information through modem 31 and communication link 106 to broadcasting station 101 which checks the identification information against a subscription list and determines whether the user has subscribed to the broadcasting station's service, as represented by inquiry S61. If the user is not subscribed, the broadcasting station terminates the connection with receiving system 102A in step S62.

If the user is subscribed, inquiry S61 is answered in the affirmative and operation continues to inquiry S63, which polls the user to determine whether or not the video program is to be purchased. If the user enters an affirmative response into user interface 30, operation proceeds to inquiry S64. Otherwise, operation proceeds to inquiry S65.

At inquiry S64, the broadcasting station 101 determines whether the user has prepaid for the video program and if not, the user is further queried to determine if payment will be made at that time. If the price of the video program has been previously paid or is immediately paid, then processing proceeds with step S66. Otherwise, processing proceeds with step S67.

In step S66, broadcasting station 101 transmits the video program via satellite to antenna 103 and transmits the FULL ACCESS signal via communication link 106 and modem 31 to access controller 28A. Access controller 28A disables encipherer 22, allowing the video program to be recorded in an unencrypted form on storage

ISDOCID: <EP_____0691787A1_I_>

IPR2025-00305
ASUS EX1002 Page 267

medium 40, and the access controller also stores the FULL ACCESS signal in access condition memory 29.

In step S67, broadcasting station 101 transmits the video program via satellite to antenna 103 and transmits the NO REPRO signal via communication link 106 and modem 31 to access controller 28A. The access controller enables encipherer 22, causing the video program to be encrypted and then recorded in encrypted form on storage medium 40, and the NO REPRO signal is stored in access condition memory 29.

If the video program is not to be purchased, resulting in a negative answer to inquiry S63, the operation proceeds to inquiry S65 whereat the user is polled to determine whether the video program is to be rented for a number (N) of viewings. If the user enters an affirmative response into user interface 30, the number N is entered, and operation proceeds to inquiry S69. Otherwise, operation proceeds to inquiry S68.

At inquiry S69, the broadcasting station 101 determines whether the user has prepaid for the N viewings of the video program and if not, the user is further queried to determine if payment will be made at that time. If the fee for N viewings of the video program has been previously paid or is immediately paid, processing proceeds with step S71. Otherwise, processing proceeds with step S72.

In step S71, broadcasting station 101 transmits the video program via satellite to antenna 103 and transmits the REPRO N TIMES signal via communication link 106 and modem 31 to access controller 28A. The access controller 28A enables encipherer 22, causing the video program to be encrypted and then recorded on storage medium 40; and the REPRO N TIMES signal is stored in access condition memory 29.

In step S72, broadcasting station 101 transmits the video program via satellite to antenna 103 and transmits the NO REPRO signal via communication link 106 and modem 31 to access controller 28A. The access controller enables encipherer 22, causing the video program to be encrypted and then recorded on storage medium 40; and the NO REPRO signal is stored in access condition memory 29.

If the video program is not to be rented for N viewings, inquiry S65 is answered in the negative and the operation proceeds to inquiry S68 whereat the user is polled to determine whether a video program is to be rented for viewing until a date Y. If the user enters an affirmative response into user interface 30, the date Y is entered, and operation proceeds to inquiry S70. Otherwise, operation returns step S62, described above.

At inquiry S70, the broadcasting station 101 determines whether the user has prepaid for the rental of the video program until date Y and if not, the user is further queried to determine if payment will be made at that time. If the fee for the rental period has been previously paid or is immediately paid, then processing proceeds with step S73. Otherwise, processing proceeds with step S72, described above.

In step S73, broadcasting station 101 transmits the video program via satellite to antenna 103 and transmits the REPRO UNTIL DATE Y signal via communication link 106 and modem 31 to access controller 28A. The access controller enables encipherer 22, causing the video program to be encrypted and then recorded in encrypted form on storage medium 40. Access controller 28A also stores the REPRO UNTIL DATE Y signal in access condition memory 29.

Fig. 7 is a flow diagram of a preferred mode of operation of receiving system 102A of Fig. 2 wherein a user seeks to reproduce a selected previously recorded video program. The user initiates the process by supplying a request to reproduce a prerecorded video program at user interface 30 and the process begins at step S80, where access controller 28A retrieves from access condition memory 29 the access-control signal corresponding to the selected video program. The process proceeds to inquiry S81 whereat the access controller determines if the access-control signal is the NO REPRO signal. If so, processing proceeds with step S86; otherwise, processing proceeds to inquiry S82.

In step S86, access controller 28A causes modem 31 to connect to broadcasting station 101 and transmits identification information and program information to the broadcasting station. Processing then proceeds to inquiry S88 which queries the user to determine if payment of the full purchase price for the video program will be made at that time. If the purchase price of the video program is paid, then processing proceeds with step S93. Otherwise, processing proceeds to inquiry S89.

In step S93, broadcasting station 101 transmits the REPRO OK signal via communication link 106 and modem 31 to access controller 28A which stores the REPRO OK signal in access condition memory 29, replacing the NO REPRO signal, and processing proceeds to step S97. In step S97, the access controller enables decipherer 25; and the selected video program which is reproduced from storage medium 40 is decrypted by decipherer 25, decoded by decoder 26, and supplied for display to video display 105.

If the retrieved access-control signal is not the NO REPRO signal, as represented by a negative answer to inquiry S81, inquiry S82 determines whether the access-control signal is the REPRO N TIMES signal. If so, processing proceeds with step S94. Otherwise, processing proceeds to inquiry S83. In step S94, access controller 28A decrements N by one, debiting the single reproduction which will immediately follow. Further, the REPRO N-1 TIMES signal is stored in access condition memory 29, replacing the access-control signal previously stored there, and processing proceeds to step S97 to reproduce and decrypt the video signal, described above.

If the retrieved access-control signal is not the REPRO N TIMES signal, inquiry S83 is made to determine if the access-control signal is the REPRO UNTIL DATE Y signal. If so, processing proceeds to inquiry S87. Oth-

EX1002 - Page 268
IPR2025-00305
ASUS EX1002 Page 268

erwise, processing proceeds to inquiry S84. Inquiry S87 compares the date signal supplied by clock 27, indicating the current date, with date Y. If the current date is prior to date Y, then processing proceeds to step S97, described above. Otherwise, processing proceeds to step S90, whereat access controller 28A determines that the applicable condition has not been satisfied and therefore no video signal reproduction is authorized. The access controller thereafter terminates the connection with broadcasting station 101.

If the retrieved access-control signal is neither the NO REPRO nor the REPRO N TIMES nor the REPRO UNTIL DATE Y signal, inquiry S84 determines if the access-control signal is the REPRO OK signal. If it is, processing proceeds with step S97, described above. Otherwise, processing advances to inquiry S85 whereat access controller 28A determines if the access-control signal is the FULL ACCESS signal. If so, processing proceeds with step S96. Otherwise, processing proceeds with step S92.

In step S92, access controller 28A determines that it has failed to recognize the particular access-control signal stored in condition access memory 29, if any. Lacking a recognizable access-control signal, no video signal reproduction is authorized. Access controller 28A terminates the connection with broadcasting station 101. It should be appreciated that step S92 can be replaced with additional access-control signal definitions to provide further processing and access-control signal permutations.

In step S96, access controller 28A disables decipherer 25, and recording/reproducing section 23A reproduces the selected video program from storage medium 40. The reproduced video program passes through decipherer 25 for decoding by decoder 26, and is supplied to video display 105 for display.

If the retrieved access-control signal is the NO REPRO signal and payment of the full purchase price is not made, inquiry S88 is answered in the negative and the process advances to inquiry S89, which queries the user to determine if the fee for N viewings of the video program will be paid. If the fee for N viewings of the video program is paid, then broadcasting station 101 transmits the REPRO N TIMES signal via communication link 106 and modem 31 to access controller 28A, and processing proceeds with step S94, described above. Otherwise, processing proceeds to inquiry S91 which queries the user to determine if the fee for rental of the video program until date Y will be paid. If the fee for such a rental is paid, then processing proceeds with step S95. Otherwise, processing proceeds with step S90, described above.

In step S95, broadcasting station 101 transmits the REPRO UNTIL DATE Y signal via communication link 106 and modem 31 to access controller 28A which stores the REPRO UNTIL DATE Y signal in access condition memory 29, replacing the NO REPRO signal, and processing proceeds to step S97, described above.

Those of ordinary skill in the art will readily appreciate the modifications to be made to the flow diagrams of Figs. 6 and 7 to control the operation of the controlled-access broadcast video signal recording systems shown in Figs. 3, 4 and 5. Hence, in the interest of brevity, further description of such modified flow diagrams is not made.

Although illustrative embodiments of the present invention and modifications thereof have been described in detail herein, it is to be understood that this invention is not limited to these precise embodiments and modifications, and that other modifications and variations may be effected therein by one skilled in the art. For example, it is contemplated that a broadcast video program can be processed by an apparatus embodying the present invention for display to a user without a preceding or simultaneous recording of the video program.

Claims

1. Apparatus for receiving, recording, and reproducing data signals, comprising:
   receiving means for receiving said data signals and an access-control signal;
   processing means, coupled to said receiving means, for processing said data signals to produce processed data signals;
   control means for controlling said processing means as a function of said access-control signal;
   storage means for storing said processed data signals and for storing said access-control signal;
   means for reproducing said stored processed data signals to produce reproduced data signals and for retrieving said stored access-control signal; and
   reprocessing means coupled to said control means for reprocessing said reproduced data signals as a function of said retrieved access-control signal.

2. Apparatus according to claim 1 wherein said data signals are digital video data signals.

3. Apparatus according to claim 1 wherein said receiving means receives said data signals and said access-control signal from a broadcasting station.

4. Apparatus according to claim 1 wherein said receiving means further comprises a tuner for receiving broadcast signals.

5. Apparatus according to claim 4 wherein said receiving means further comprises a modem for receiving said access-control signal.

6. Apparatus according to claim 1 wherein said receiving means further comprises a modem for receiving said access-control signal.

7. Apparatus according to claim 1 wherein said receiv-

SDOCID: <EP_____0691787A1_I_>

EX1002 - Page 269
IPR2025-00305
ASUS EX1002 Page 269

ing means further comprises a user interface for receiving said access-control signal from a user.

8. Apparatus according to claim 1 wherein said processing means comprises a descrambler and wherein said reprocessing means comprises a descrambler.

9. Apparatus according to claim 1 wherein said processing means comprises a descrambler and an encipherer and wherein said reprocessing means comprises a decipherer.

10. Apparatus according to claim 1 wherein said processing means comprises an encipherer and wherein said reprocessing means comprises a decipherer.

11. Apparatus according to claim 1 wherein said processed data signals are stored on a record medium and said access-control signal is stored in a separate storage medium.

12. Apparatus according to claim 11 wherein said record medium is a video tape.

13. Apparatus according to claim 11 wherein said separate storage medium is an integrated circuit memory.

14. Apparatus according to claim 1 wherein said processed data signals and said access-control signal both are stored on a common record medium.

15. Apparatus according to claim 1 further comprising a clock, coupled to said receiving means and to said control means, for supplying a clock signal to said control means;

wherein said data signals include a clock reference signal; and

wherein said clock signal is synchronized with said clock reference signal.

16. Apparatus according to claim 1 further comprising a decoder, coupled to said reprocessing means, for decoding said reprocessed data signals.

17. Apparatus for receiving and recording data signals, comprising:

receiving means for receiving said data signals and an access-control signal;

processing means, coupled to said receiving means, for processing said data signals to produce processed data signals;

control means for controlling said processing means as a function of said access-control signal; and

storage means for storing said processed data signals and said access-control signal.

18. Apparatus according to claim 17 wherein said processing means comprises a descrambler.

19. Apparatus according to claim 18 wherein said processing means further comprises an encipherer.

20. Apparatus according to claim 17 wherein said processing means comprises an encipherer.

21. Apparatus according to claim 17 wherein said storage means comprises a storage cassette.

22. Apparatus according to claim 21 wherein said storage cassette contains a record medium on which said processed data signals are recorded and an integrated circuit memory in which said access-control signal is stored.

23. Apparatus for reproducing processed data signals, comprising:

means for reproducing stored processed data signals to produce reproduced data signals and for retrieving a stored access-control signal;

reprocessing means for reprocessing said reproduced data signals to produce reprocessed data signals; and

control means for controlling said reprocessing means as a function of said retrieved access-control signal.

24. Apparatus according to claim 23 wherein said reprocessing means comprises a descrambler.

25. Apparatus according to claim 23 wherein said reprocessing means comprises a decipherer.

26. Apparatus according to claim 23 wherein said processed data signals and said access-control signals are stored in a storage cassette.

27. A method for transferring from a broadcaster to a receiver a limited reproduction right in data, comprising the steps of:

transmitting from said broadcaster to said receiver an access-control signal and said data, said access-control signal indicating said limited reproduction right;

receiving, at said receiver, said access-control signal and said data;

processing, at said receiver, said data as a function of said access-control signal to produce processed data;

storing, at said receiver, said processed data and said access-control signal;

retrieving, at said receiver, said stored access-control signal;

EX1002 - Page 270
IPR2025-00305
ASUS EX1002 Page 270

reproducing, at said receiver, said stored processed data to produce reproduced data; and

reprocessing, at said receiver, said reproduced data as a function of said retrieved access-control signal.

28. The method, according to claim 27, wherein said limited reproduction right is the right to reproduce said data N times.

29. The method, according to claim 27, wherein said limited reproduction right is the right to reproduce said data until date Y.

30. The method, according to claim 27, wherein said limited reproduction right is the right to reproduce said data until time T.

31. The method, according to claim 27, wherein said data is transmitted in scrambled form and said step of processing said data comprises descrambling said data.

32. The method, according to claim 31, wherein said step of processing said data further comprises enciphering said data; and

wherein said step of reprocessing said reproduced data comprises deciphering said reproduced data.

33. The method, according to claim 27, wherein said step of processing said data comprises enciphering said data; and

wherein said step of reprocessing said reproduced data comprises deciphering said reproduced data.

34. The method, according to claim 27, wherein said data is transmitted and stored in scrambled form, and said step of reprocessing said reproduced data comprises descrambling said reproduced data.

35. The method, according to claim 27, wherein said processed data and said access-control signal are stored on a storage cassette.

36. A method for transferring from a broadcaster to a receiver a limited reproduction right in prerecorded data, comprising the steps of:

transmitting from said broadcaster to said receiver an access-control signal, said access-control signal indicating said limited reproduction right;

receiving, at said receiver, said access-control signal;

reproducing, at said receiver, said prerecorded data; and

processing, at said receiver, said reproduced data as a function of said access-control signal.

37. The method, according to claim 36, wherein said step of processing said reproduced data comprises deciphering said reproduced data.

38. The method, according to claim 36, wherein said step of processing said reproduced data comprises descrambling said reproduced data.

39. A method for reproducing prerecorded data comprising the steps of:

reproducing an access-control signal from a first storage medium;

reproducing processed data from a second storage medium as a function of said access-control signal to produce reproduced data; and

reprocessing said reproduced data as a function of said access-control signal.

40. A method for erasing prerecorded data stored on a record medium as a function of an access-control signal stored in a separate memory, comprising the steps of:

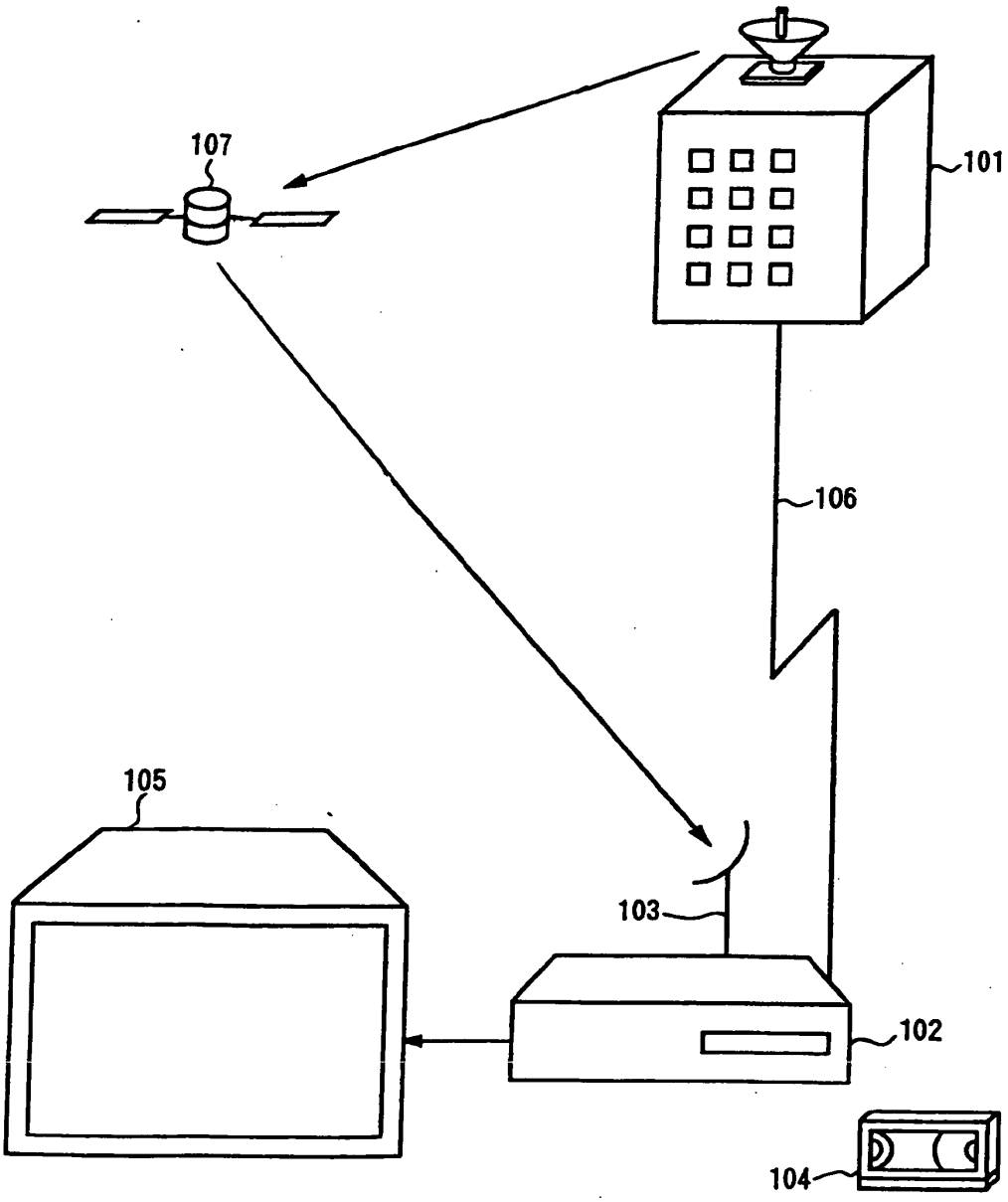
retrieving said access-control signal from said separate memory;

recognizing said access-control signal as an ERASE signal; and

erasing data stored on said record medium in response to an ERASE signal.

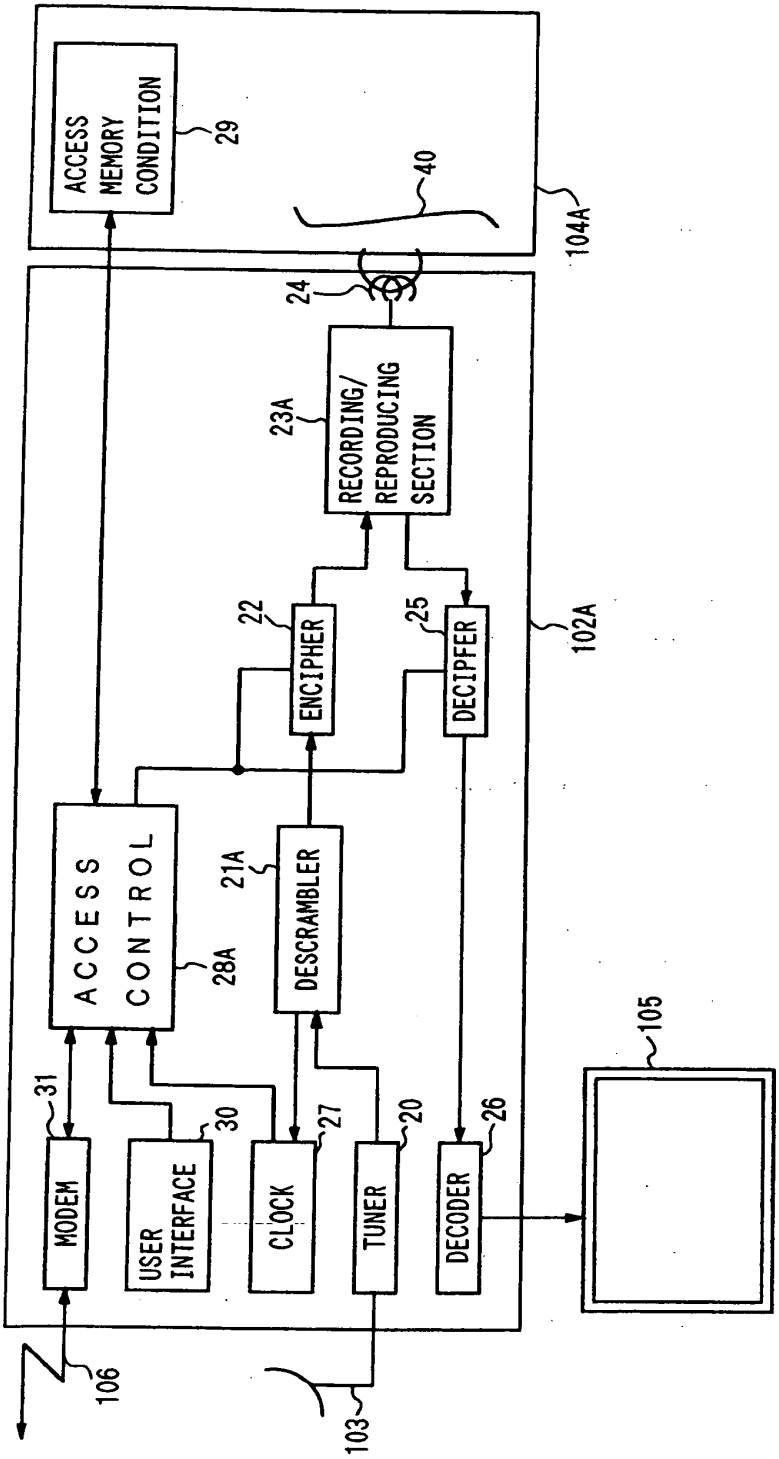
EX1002 - Page 271
IPR2025-00305
ASUS EX1002 Page 271

Fig. 1



EX1002 - Page 272
IPR2025-00305
ASUS EX1002 Page 272

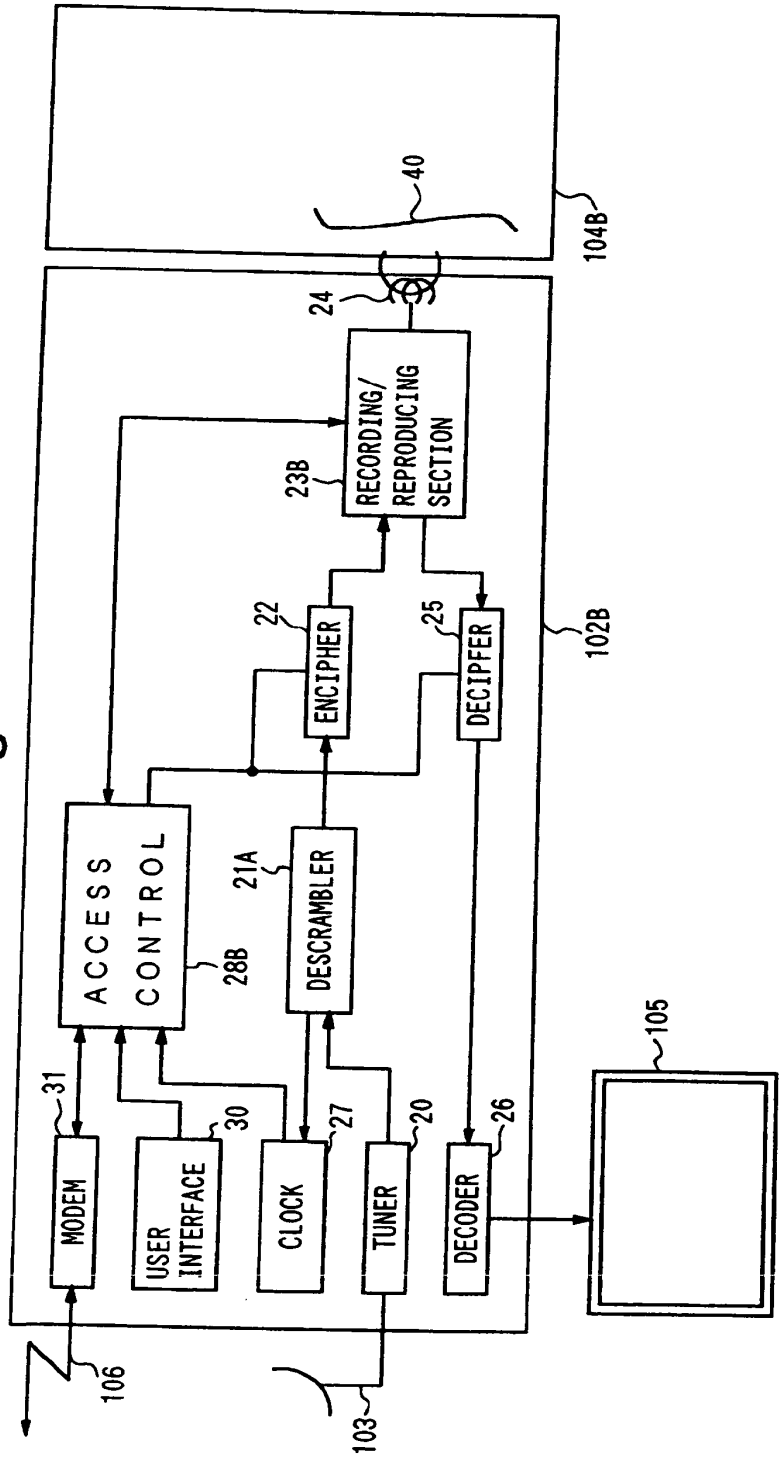
Fig. 2



SDOCID: <EP_____0691787A1_I_>

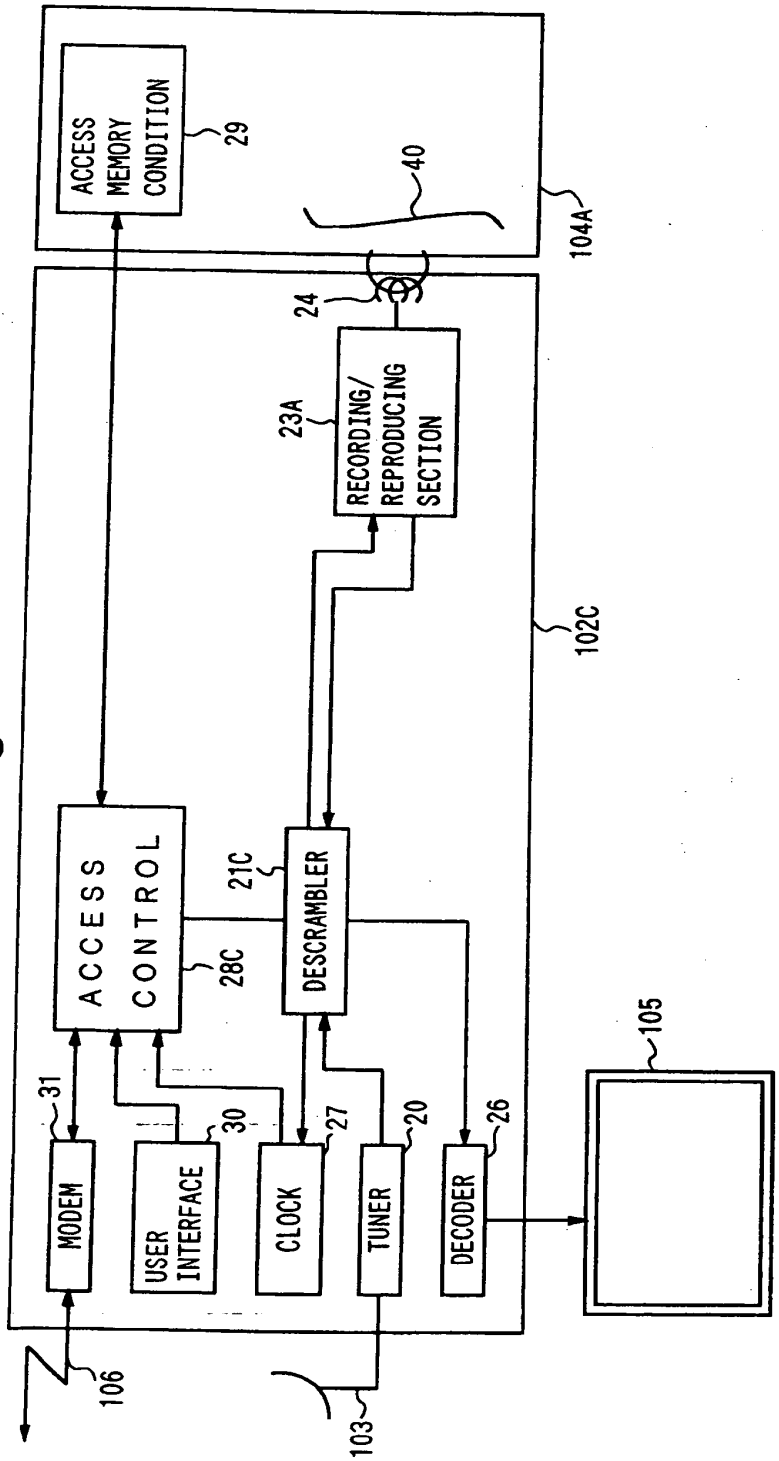
IPR2025-00305
ASUS EX1002 Page 273

Fig. 3



IPR2025-00305
ASUS EX1002 Page 274

Fig. 4



SDOCID: <EP_____0691787A1_I_>

IPR2025-00305
ASUS EX1002 Page 275

Fig. 5

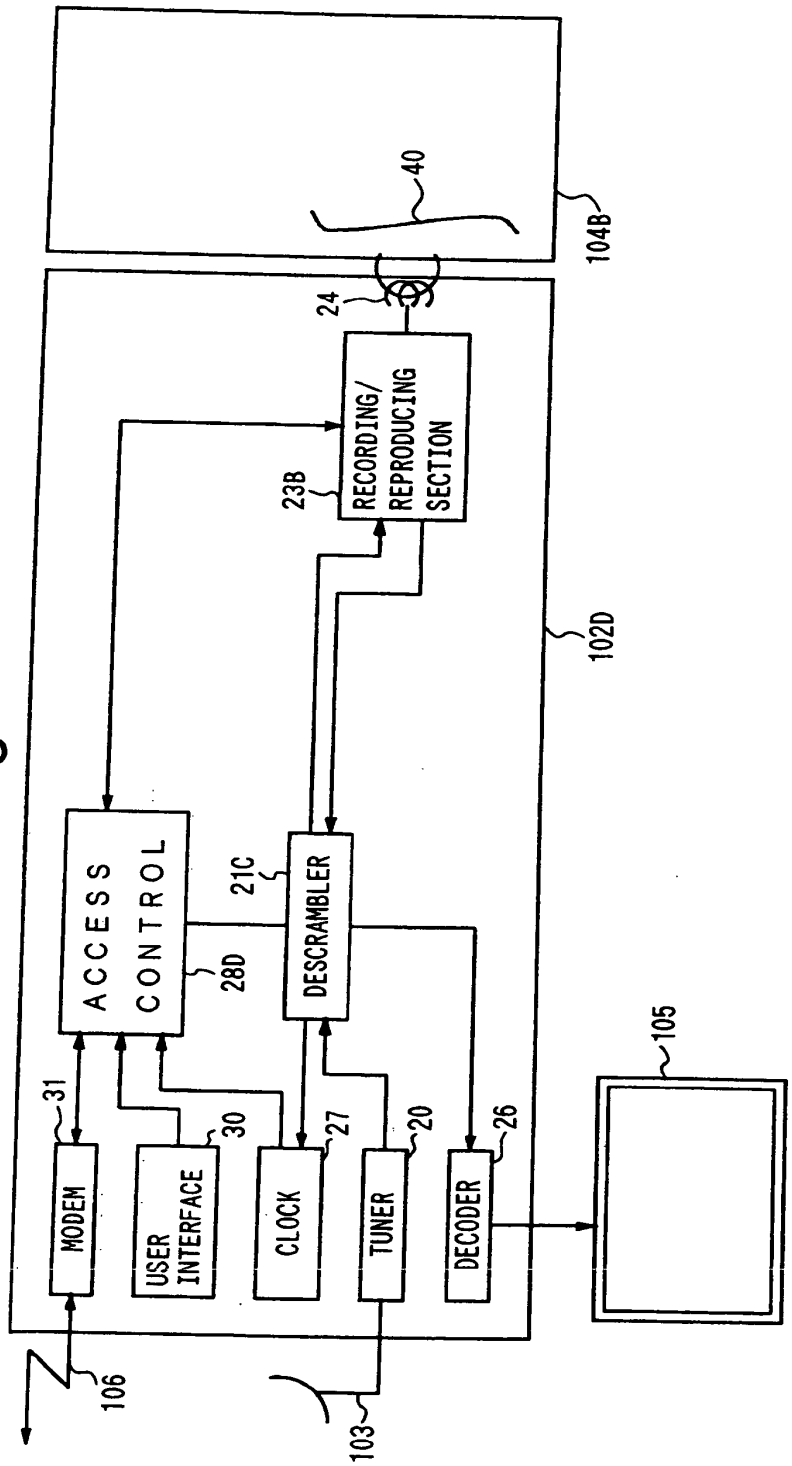
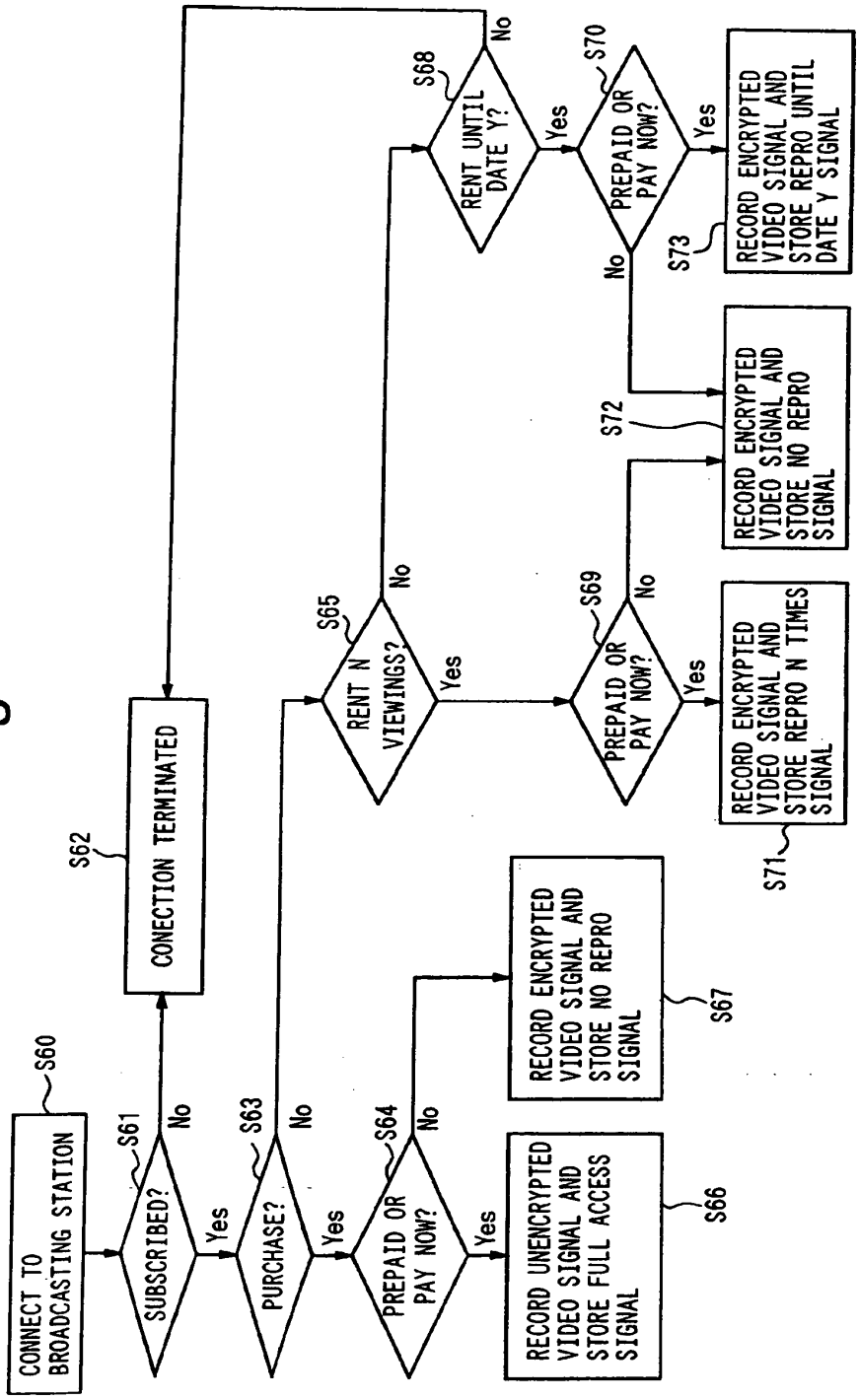

40
104B
24
RECORDING/
REPRODUCING
SECTION
23B
102D
ACCESS
CONTROL
28D
21C
DESCRAMBLER
105
31
30
27
20
26
MODEM
USER
INTERFACE
CLOCK
TUNER
DECODER
106
103

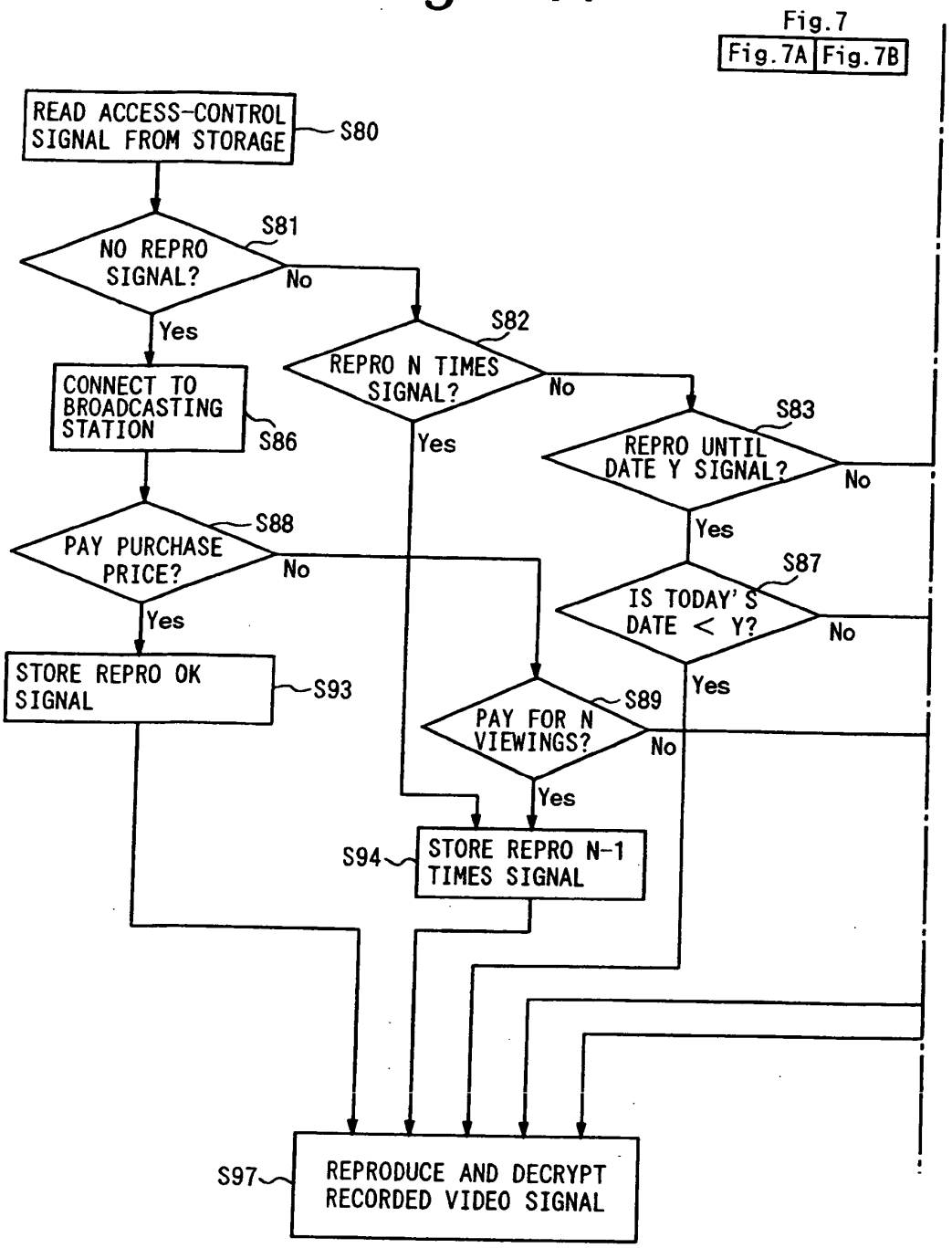
Fig. 6



EDOCID: <EP _0691787A1_I_>

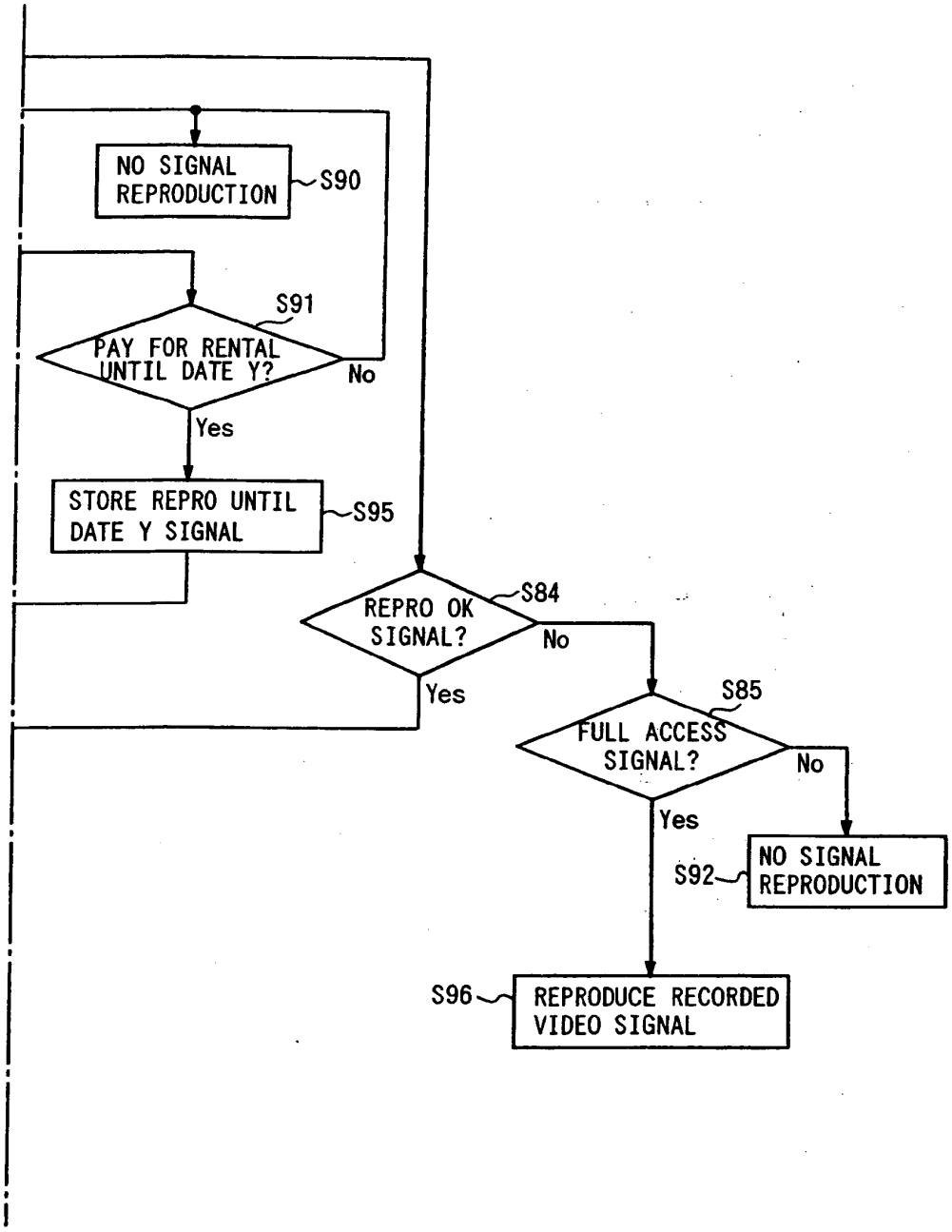
EX1002 - Page 277
IPR2025-00305
ASUS EX1002 Page 277

Fig. 7A



EX1002 - Page 278
IPR2025-00305
ASUS EX1002 Page 278

Fig. 7B



SDOCID: <EP_____0691787A1_I_>

IPR2025-00305
ASUS EX1002 Page 279

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 30 4743

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X Y	US-A-5 054 064 (WALKER STEPHEN S ET AL) 1 October 1991 * the whole document * ---	1-12,14, 16-21, 23-27, 31-39 22	H04N5/913 H04N7/167
X Y	DE-A-43 34 931 (MITSUBISHI CORP) 28 April 1994 * column 3, line 40 - column 5, line 22 * * column 9, line 25 - column 17, line 26 * * figures 1,6-16 * ---	1-13, 17-21, 23-25, 27, 31-34, 36-39 22	
P,X	US-A-5 400 402 (GARFINKLE NORTON) 21 March 1995 * the whole document * ---	1,2, 8-21, 23-40	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
X	EP-A-0 267 039 (SATELLITE TECHNOLOGY SERVICES) 11 May 1988 * page 2, column 2, line 28 - column 4, line 38 * * figure 1 * -----	1-6,8, 27,31	H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	16 October 1995	Van der Zaal, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

OIPE
MAY 03 2006
PATENT & TRADEMARK OFFICE
1AP100

Atty. Docket No. 006517.P002 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Luc Vantalon, *et al.*

Application No. 11/007,116

Filed: December 7, 2004

For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

Examiner: Not yet assigned.

Art Unit: 2131

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

INFORMATION DISCLOSURE STATEMENT

Sir:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 together with copies of the documents cited on that form, except for copies not required to be submitted (e.g., copies of U.S. patents and U.S. published patent applications need not be enclosed). It is respectfully requested that the cited documents be considered and that the enclosed copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Pursuant to 37 C.F.R. § 1.97, this Information Disclosure Statement is being submitted under one of the following (as indicated by an "X" to the left of the appropriate paragraph):

_____ 37 C.F.R. §1.97(b).

IPR2025-00305
ASUS EX1002 Page 281

__X__ 37 C.F.R. §1.97(c). If so, then enclosed with this Information Disclosure Statement is one of the following:

__X__ A statement pursuant to 37 C.F.R. §1.97(e) or

____ A check for $_____ for the fee under 37 C.F.R. § 1.17(p).

_____ 37 C.F.R. §1.97(d). If so, then enclosed with this Information Disclosure Statement are the following:

(1) A statement pursuant to 37 C.F.R. §1.97(e); and

(2) A check for $_____ for the fee under 37 C.F.R. §1.17(p) for submission of the Information Disclosure Statement.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 5/1, 2006

James C. Scheller, Jr.
Reg. No. 31,195

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8300

FIRST CLASS CERTIFICATE OF MAILING (37 C.F.R. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on: May 1, 2006.

Date of Deposit

Cathi L.G. Thoorsell

Name of Person Mailing Correspondence

Cathi L.G. Thoorsell — Signature

May 1, 2006 — Date

IPR2025-00305
ASUS EX1002 Page 282

Substitute for Form 1449/PTO			Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*			Application Number	11/007,116
			Filing Date	December 7, 2004
			First Named Inventor:	Luc Vantalon
			Art Unit	2131
			Examiner Name	
Sheet 1	of	2	Attorney Docket No.	006517.P002

OIPE MAY 0 3 2006 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Exmnr Initials*	Cite No.[1]	Document Number: Number	Document Number: Kind Code[2] (If known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US-2003/196092	A1	10-16-2003	Raley, M., *et al.*	

FOREIGN PATENT DOCUMENTS

Exmnr Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	2	FR 2 843 257 A1	02-06-2004	Viaccess		
	3	WO 03/010722 A2	02-06-2003	SCM Microsystems GMBH		
	4	EP 0 858 184 A2	08-12-1998	NDS Limited		
	5	WO 00/56068 A1	09-21-2000	Thomson Licensing S.A.		
	6	EP 0 691 787 A1	01-10-1996	Sony Corporation		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08A (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.

IPR2025-00305
ASUS EX1002 Page 283

Substitute for Form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	11/007,116
				Filing Date	December 7, 2004
				First Named Inventor:	Luc Vantalon
				Art Unit	2131
				Examiner Name	
Sheet	2	**of**	2	Attorney Docket No.	006517.P002

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	7	VAN MOFFAERT, A., *et al.,* "Digital Rights Management: DRM is a key enabler for the future growth of the broadband access market, and the telecom/networking market in general." Alcatel Telecommunications Review, Alcatel, Paris Cedex, FR, April 2003 (2003-2004), XP007005930 ISSN: 1267-7167, pages 1-7.	
	8	International Search Report and Written Opinion of the International Searching Authority for PCT/US2005/039794, mailed April 3, 2006, 11 pages.	

Examiner Signature		Date Considered	

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08B (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.

OIPE
MAY 03 2006
PATENT & TRADEMARK OFFICE

Atty. Docket No. 006517.P002

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Application of:

Luc Vantalon, *et al.*

Application No. 11/007,116

Filed: December 7, 2004

For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

Examiner: Not yet assigned.

Art Unit: 2131

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, PO Box 1450, Alexandria, Virginia 22313-1450

on 05-01-2006
Date of Deposit

Cathi L. G. Thoorsell
Name of Person Mailing Correspondence

Cathi L. G. Thoorsell May 1, 2006
Signature Date

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

STATEMENT UNDER 37 C.F.R. §1.97(e)

Sir:

I hereby certify (as indicated by an "X" to the left of the appropriate paragraph):

X That each item of information contained in the accompanying Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement.

____ That no item of information contained in the accompanying Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned attorney after making reasonable inquiry, no item of information contained in the Information Disclosure Statement was known to any individual designated in §1.56(c) more than three months prior to the filing the Information Disclosure Statement.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 5/1, 2006

James C. Scheller, Jr.
Reg. No. 31,195

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8300

IPR2025-00305
ASUS EX1002 Page 285

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	
Luc Vantalon, et al.	Examiner: Brian E. Weinrich
Application No.: 11/007,116	Art Unit: 4193
Filed: December 7, 2004	Confirmation No.: 9254
For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

INFORMATION DISCLOSURE STATEMENT

Sir:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 together with copies of the documents cited on that form, except for copies not required to be submitted (e.g., copies of U.S. patents and U.S. published patent applications need not be enclosed for applications filed after June 30, 2003). It is respectfully requested that the cited documents be considered and that the enclosed copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Pursuant to 37 C.F.R. § 1.97, this Information Disclosure Statement is being submitted under one of the following (as indicated by an "X" to the left of the appropriate paragraph):

X 37 C.F.R. §1.97(b).

_____ 37 C.F.R. §1.97(c). If so, then enclosed with this Information Disclosure Statement is one of the following:

_____ A statement pursuant to 37 C.F.R. §1.97(e) or

_____ A check for $180.00 for the fee under 37 C.F.R. § 1.17(p).

_____ 37 C.F.R. §1.97(d). If so, then enclosed with this Information Disclosure Statement are the following:

(1) A statement pursuant to 37 C.F.R. §1.97(e); and

(2) A check for $180.00 for the fee under 37 C.F.R. §1.17(p) for submission of the Information Disclosure Statement.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: October 24, 2007

James C. Scheller, Jr.
Reg. No. 31.195

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

October 24, 2007.
Date of Deposit

Name of Person Filing Correspondence

Signature

October 24, 2007
Date

Substitute for Form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	11/007,116
				Filing Date	December 7, 2004
				First Named Inventor:	Luc Vantalon, et al.
				Art Unit	4193
				Examiner Name	Brian E. Weinrich
Sheet	1	**of**	1	Attorney Docket Number	6517.P002

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	1	PCT Notification Concerning Transmittal of Copy of International Preliminary report on Patentability, Date June 21, 2007, 7 Pages.	

Examiner Signature		Date Considered	

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08A (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.

Electronic Acknowledgement Receipt

EFS ID:	2366320
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	James Scheller Jr./Cathi Thoorsell
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	6517P002
Receipt Date:	24-OCT-2007
Filing Date:	07-DEC-2004
Time Stamp:	20:02:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	6517P002_IDS.PDF	140652 5933f029ccec19817aacbc35d324de6483911556	no	3
Warnings:					

IPR2025-00305
ASUS EX1002 Page 289

Information:					
This is not an USPTO supplied IDS fillable form					
2	NPL Documents	6517P002_IDS_Ref_1.PDF	294218 3517436203b8310203b2bcdabc0f7478c8f64626	no	7
Warnings:					
Information:					
			Total Files Size (in bytes):	434870	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Atty. Docket No. 06517.P002 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Luc Vantalon, et al.	)	Examiner: Avery, Jeremiah L.
	)	
Application No. 11/007,116	)	Art Unit: 2431
	)	
Filed: December 7, 2004	)	
	)	Confirmation No. 9254
For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

STATUS INQUIRY UNDER MPEP 203.08

Sir:

Applicant respectfully requests information concerning the status of this application. No correspondence has been received from the Patent and Trademark Office since the Notice of Publication dated June 8, 2006.

Please provide to the Applicant, by written response, an expected date of when the Examiner will take action on this application.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: Nov. 13, 2008

James C. Scheller, Jr.
Reg. No. 31,195

1279 Oakmead Parkway
Sunnyvale, CA 94085
(408) 720-8300

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

November 13, 2008
Date of Deposit

Connie Thayer
Name of Person Filing Correspondence

Connie Thayer 11-13-08
Signature Date

IPR2025-00305
ASUS EX1002 Page 291

Electronic Acknowledgement Receipt	
EFS ID:	4287774
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	08791
Filer:	James Scheller Jr./Connie Thayer
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	6517P002
Receipt Date:	13-NOV-2008
Filing Date:	07-DEC-2004
Time Stamp:	20:30:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for status of Application	6517P002_Status_Inquiry.PDF	69116 36658ca5ee7df9cf83a6086a8eaace422c715d21	no	1
Warnings:					
Information:					

IPR2025-00305
ASUS EX1002 Page 292

Total Files Size (in bytes):	69116

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

8791 7590 11/18/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
11/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

DATE: 11/14/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

To: Applicant of Serial Number 11007116
Filed on 07-DEC-2004
(Art Unit 2431)

It is estimated that this application will receive an Office action in approximately 3 months. This is an estimate that is based on the current inventory level of applications filed in this art area and the current staffing levels in this Art Unit. The USPTO is dedicated to minimizing first action and total pendency, and we are targeting resources to help address backlogs in art areas with high new application filings. Thank you for your inquiry.

Customer Service Office in Technology Center: 2400

Phone Number: 571-272-2400
Central Fax Number: 571-273-8300

Applicant/Attorney Contact Information:

Phone Number:
Fax Number:

PTOLFA1 (Rev. 07/05)

IPR2025-00305
ASUS EX1002 Page 295

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

8791 7590 04/01/2009

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/007,116	VANTALON ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-146* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-146* is/are rejected.

7)☒ Claim(s) *24,25,101,136 and 146* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-146 have been examined.

Claim Objections

1. Claims 24 and 25 are objected to because of the following informalities: punctuation error. There is a period (.) in the middle of the claims, where either a comma or semi-colon should be. It can be interpreted that the first period marks the end of claims 24 and 25. Appropriate correction is required.

2. Claim 101 is objected to because of a spelling error. The word “messags” should be “messages”. Appropriate correction is required.

3. Claim 136 is objected to because of a repeated instance of the word "to". The claim language of "the processor is to to generate" is erroneous and appropriate correction is required.

4. Claim 146 is objected to due to a grammatical error. The claim language “an physical interface” should be “*a* physical interface”. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-35, 37-40, 4-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132, 134-136, 137, 140-143 and 146 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent No. 7,036,011 to Grimes et al., hereinafter Grimes.

5. Regarding claim 1, Grimes teaches a method to control a presentation of content, the method comprising:

receiving a representation of content from a first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access (column 2, lines 1-31, “content is encrypted with an encryption key”);

presenting the content, at a user's request, through a second conditional access server which is coupled to the first conditional access server (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

wherein the presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”);

IPR2025-00305
ASUS EX1002 Page 299

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content (column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

6. Regarding claim 2, Grimes teaches wherein the content is presented by a network client of the second conditional access server using the second set of cryptographic keys (column 4, lines 20-28, column 5, lines 50-56, column 6, lines 35-52, “encrypting and transmitting the encryption key 98” and column 7, lines 30-51).

7. Regarding claim 3, Grimes teaches wherein the first conditional access server provides the second conditional access server the first set of cryptographic keys for authorized use (column 5, lines 50-56, column 6, lines 35-52, column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62 and column 9, lines 38-60).

8. Regarding claim 4, Grimes teaches wherein the user's request is after the first conditional access server provides at least a portion of the content; and the portion of the content is presented in response to the user's request (column 7, lines 11-29, “only

those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate").

9. Regarding claims 5 and 14, Grimes teaches wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the network client is a digital rights management client (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

10. Regarding claims 6 and 14, Grimes teaches wherein the second conditional access server authorizes the network client to use the content through the digital rights management system in accordance with authorization to use received from the first conditional access server (column 7, lines 11-29, "only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate").

11. Regarding claims 7 and 20, Grimes teaches wherein the second conditional access server translates authorization to access the content from authorization received from the first conditional access server to authorization for the network client (column 7, lines 11-29, "only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate").

12. Regarding claims 8, 17 and 27, Grimes teaches wherein the second set of cryptographic keys consists one key (column 2, lines 1-31, "content is encrypted with an encryption key").

13. Regarding claim 9, Grimes teaches wherein the second conditional access server acts as a primary conditional access server to another secondary conditional access server (column 7, lines 18-23, “the DRM server 58 or other server at the NOC 12”, column 8, lines 16-31, “third-party website server” and column 9, lines 3-11).

14. Regarding claim 10, Grimes discloses a machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content, the method comprising:

receiving, at a second conditional access server, a first set of cryptographic keys from a first conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

authorizing a client of the second conditional access server to present the content in accordance with authorization the second conditional access server received from the first conditional access server (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”);

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content (column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and

the content may be encrypted so that only clients 18 that receive the digital certificate can access the content", column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

15. Regarding claim 11, Grimes discloses wherein the method further comprises: recording a representation of the content in an encrypted form in response to a message from the first conditional access server (column 2, lines 10-21, column 6, lines 35-52, column 7, lines 30-51, column 8, lines 16-31 and 51-62, column 9, lines 3-20, column 10, lines 19-29 and 37-46 and column 11, lines 26-47).

16. Regarding claim 12, Grimes discloses wherein the client sends a request, through a network connection to the second conditional access server, for authorization to present the content after the first conditional access server provides at least a portion of the content which is recorded; the second conditional access server obtains authorization from the first conditional access server, after the first conditional access server provides the portion of the content, for said authorizing (column 7, lines 11-29, "if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content", column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

17. Regarding claim 13, Grimes discloses wherein the method further comprises: translating authorization to access the content from authorization received from the first conditional access server to authorization for the client (column 7, lines 11-29, "only

those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate").

18. Regarding claim 16, Grimes discloses wherein the first conditional access server provides authorization to the second conditional access server according to an identity of the second conditional access server; the second conditional access server provides authorization to the client according to an identity of the client (column 3, lines 29-41, column 7, lines 11-29, "if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content", column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18);

the first conditional access server is not aware of an identity of the client (column 7, lines 40-51, "generating a digital certificate 84 may be performed by the third-party website server (e.g., when the user orders content from a third-party website)").

19. Regarding claim 18, Grimes discloses wherein the second conditional access server is a server of a further secondary conditional access server and acts as a primary conditional access server with respect to the further secondary conditional access server (column 7, lines 18-23, "the DRM server 58 or other server at the NOC 12", column 8, lines 16-31, "third-party website server" and column 9, lines 3-11).

20. Regarding claims 19 and 23, Grimes discloses a secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

IPR2025-00305
ASUS EX1002 Page 304

a communication interface, the communication interface to receive a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys (column 2, lines 10-39, “computer-readable medium further comprises instructions for requesting the encryption key from a digital rights management (DRM) server using a digital certificate”, column 4, lines 29-49, column 5, lines 53-65, column 7, lines 11-29 and column 13, lines 4-18);
a controller coupled to the communication interface, the controller to authorize a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server; wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content (column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

21. Regarding claim 21, Grimes discloses wherein the second set of cryptographic keys comprises a key of a digital rights management system; the client comprises a digital rights management client; the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server (column 2, lines

1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

22. Regarding claims 22 and 26, Grimes discloses wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of the client (column 3, lines 29-41, column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18);

the primary conditional access server is not aware of an identity of the client (column 7, lines 40-51, “generating a digital certificate 84 may be performed by the third-party website server (e.g., when the user orders content from a third-party website)").

23. Regarding claim 24, Grimes discloses means for recording a representation of the content in an encrypted form in response to a message from the primary conditional access server. wherein the client sends a request, through a network connection to the secondary conditional access server, for authorization to present the content after the primary conditional access server provides at least a portion of the content which is recorded; the secondary conditional access server obtains authorization from the

primary conditional access server, after the primary conditional access server provides the portion of the content, for authorizing the client to present the content (column 7, lines 7-29, "if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content", column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

24. Regarding claim 25, Grimes discloses means for translating authorization to access the content from authorization received from the primary conditional access server to authorization for the client. wherein the second set of cryptographic keys comprises a key of a digital rights management system; the client comprises a digital rights management client; wherein the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

25. Regarding claims 28, 62 and 96, Grimes teaches a method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component; broadcasting the media component from a first conditional access server; receiving a client request to use the media component from a

client through a second conditional access server after said broadcasting; responding to the client request through the second conditional access server (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

26. Regarding claims 29, 63 and 97, Grimes teaches broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request (column 7, lines 7-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

27. Regarding claims 30, 64 and 98, Grimes teaches wherein the client is not authorized to use the portion of the media content before the second entitlement management message (column 11, lines 3-19, "validation refused" and column 13, lines 4-18, "the hardware profile will not match the user machine 40 of client 18 if the user has made an unauthorized transfer of the client software 43").

28. Regarding claims 31, 65 and 99, Grimes teaches wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously (column 3, lines 61-67, column 4, lines 1-9, “this stored or personal content 28 may be kept on a user machine hard-drive or other storage medium” and 42-59 and column 5, lines 1-18).

29. Regarding claims 32, 66, 100 and 130, Grimes teaches a method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

processing the security messages on the conditional access server (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

30. Regarding claims 33, 67 and 101, Grimes teaches wherein the security messages comprise entitlement management messages;

the conditional access server has a user key representing a subscriber of the primary security system (column 6, lines 65-67, column 7, lines 1-29 and column 8, lines 43-50);

said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system (column 9, lines 24-60).

31. Regarding claims 34, 68 and 102, Grimes teaches wherein the access controlled data is protected using a digital rights management system (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-

22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

32. Regarding claims 35, 69, 103 and 132, Grimes teaches wherein rights to the access controlled data are at least partially derived from the entitlement management messages (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

33. Regarding claims 38, 72, 106 and 134, Grimes teaches receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system (column 12, lines 26-61 and column 13, lines 19-25 and 28-30); descrambling the scrambled content according to the entitlement control message; wherein the access controlled data comprises a result of descrambling the scrambled content (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

34. Regarding claims 39, 73, 107 and 135, Grimes teaches storing, at the conditional access server, the content in an encrypted form; wherein the access controlled data is provided in response to a request from the secondary conditional access client (column 2, lines 10-21, column 6, lines 35-52, column 7, lines 30-51, column 8, lines 16-31 and 51-62, column 9, lines 3-20, column 10, lines 19-29 and 37-46 and column 11, lines 26-47).

35. Regarding claims 40, 74, 108, 136, Grimes teaches receiving, at the conditional access server, an entitlement control message of the primary security system; processing the entitlement control message on the conditional access server to

generate a substitutive entitlement control message as a replacement of the entitlement control message; wherein the access controlled data comprises the substitutive entitlement control message (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

36. Regarding claims 48, 82 and 116, Grimes teaches a method to process media content provided by a primary security system, the method comprising:

receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

37. Regarding claims 49, 83, 117 and 141, Grimes teaches wherein the security message is an entitlement message; wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system (column 7, lines 40-51, “generating a digital certificate 84 may be performed by the third-party website server (e.g., when the user orders content from a third-party website)", column 11, lines 3-19, "validation refused" and column 13, lines 4-18, "the hardware profile will not match the user machine 40 of client 18 if the user has made an unauthorized transfer of the client software 43").

38. Regarding claims 50, 84, 118 and 142, Grimes teaches wherein the access controlled format protects access to data using a digital rights management system (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

39. Regarding claims 51, 85 and 119, Grimes teaches automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data (column 12, lines 26-61 and column 13, lines 19-25 and 28-30);

descrambling and recording the portion of the media content in response to a determination to descramble (column 12, lines 62-67 and column 13, lines 1-3 and 25-28);

recording the portion of the media content without descrambling in response to a determination not to descramble (column 12, lines 26-61 and column 13, lines 19-25 and 28-30).

40. Regarding claims 57, 91 and 125, Grimes teaches wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

41. Regarding claims 58, 92 and 126, Grimes teaches receiving a first entitlement control message for descrambling a portion of media content received from the primary

security system; sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

42. Regarding claims 59, 93 and 127, Grimes teaches wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; the method further comprises: storing the second entitlement control message with the portion of the media content (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

43. Regarding claim 131, Grimes discloses wherein the security messages comprise entitlement management messages; the access controlled data is protected using a digital rights management system (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

44. Regarding claim 140, Grimes discloses a secondary conditional access client, comprising:

a communication interface to receive, from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system;

a processor coupled to the communication interface, the processor to process the access controlled data (column 7, lines 11-29, “only those clients 18 that purchased the

PPV content or the subscription, or that meet the restriction, will receive the digital certificate").

45. Regarding claim 143, Grimes discloses wherein the processor is to automatically determine whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data (column 12, lines 26-61 and column 13, lines 19-25 and 28-30);

the client further comprises:

a storage device; a descrambler coupled to the processor and the storage device, in response to a determination to descramble the descrambler to descramble the portion of the media content for storing in the storage device, in response to a determination not to descramble the storage device to record the portion of the media content without descrambling (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

46. Regarding claim 146, Grimes discloses an physical interface to receive a first entitlement control message for descrambling a portion of media content received from the primary security system (column 12, lines 62-67 and column 13, lines 1-3 and 25-28);

and wherein the communication interface is to send the first entitlement control message to the conditional access server through a network connection (column 3, lines 29-41, column 7, lines 11-29, "if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital

certificate can access the content", column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 36, 41-47, 52-56, 60, 61, 70, 75-81, 86-90, 94, 95, 104, 109-115, 120-124, 128, 129, 133, 137-139, 144 and 145 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grimes as applied to claims 32, 66, 100, 130 and 140 above, and further in view of United States Patent No. 7,302,058 to Candelore, hereinafter Candelore.

47. Grimes significantly teaches the claimed invention, as cited above. However, Grimes does not substantially teach the claim language in the following claims pertaining to "control words". Candelore teaches said claim language, as cited below.

48. The motivation to combine would be that "the control word is only decrypted in descrambler IC 440 that actually uses the control word, therefore, the control word is never exposed, and cannot be obtained by hackers". (*Candelore* – column 6, lines 42-49).

49. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Candelore with the teachings of Grimes so that "Local Access control can be performed by the Insecure Processor because the critical 'secure' function is isolated in the Descrambler IC" (*Candelore* – column 10, lines 48-54).

50. Regarding claims 36, 70, 104 and 133, Candelore teaches receiving, at the conditional access server, an entitlement control message of the primary security system (column 3, lines 61-67, column 4, lines 1-14 and 55-67 and column 5, lines 1-3 and 20-26);

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system (column 5, lines 20-26 and column 6, lines 11-31 and 42-51);

wherein the access controlled data comprises the control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, "conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content" and column 7, lines 25-41).

51. Regarding claims 37, 71 and 105, Candelore teaches wherein the access controlled data comprises a decrypted version of the entitlement control message (column 4, lines 6-14, column 6, lines 32-49 and column 7, lines 25-41).

52. Regarding claims 41, 75, 109 and 137, Candelore teaches wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server (column 3, lines 15-23, column 6, lines 11-31, “encrypts the CWs in encryption block 414 with keys that are unique to transport descrambler integrated circuit (IC) 440” and column 7, lines 54-62).

53. Regarding claims 42, 76 and 110, Candelore teaches wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system (column 4, lines 9-13 and column 6, lines 11-20 and 42-49).

54. Regarding claims 43, 77 and 111, Candelore teaches wherein the entitlement control message and the substitutive entitlement control message have a same control word (Figure 2, element 416 and Figure 3, elements 41, 44 and 45, column 3, lines 15-23, column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

55. Regarding claims 44, 78 and 112, Candelore teaches wherein the entitlement control message has a first control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, “conditional

access unit 401 will decrypt the control words and use the clear control words to descramble the program content" and column 7, lines 25-41);

the substitutive entitlement control message has a second control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

the first and second control words are different (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61).

56. Regarding claims 45, 79 and 113, Candelore teaches wherein the access controlled data further comprises the first and second control words (Figure 6, "encrypted control word A" and "encrypted control word B" and column 7, lines 42-61).

57. Regarding claims 46, 80, 114 and 138, Candelore teaches receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word (column 3, lines 15-24 and column 6, lines 14-17 and 60-63);

generating a second entitlement control message containing a second control word that is different from the first control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

descrambling the content using the first control word and rescrambling the content by the second control word (column 6, lines 11-20, column 7, lines 54-67 and column 8, lines 1-23);

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message (column 5, lines 55-65).

58. Regarding claims 47, 81 and 115, Candelore teaches storing, at the conditional access server, the content rescrambled by the second control word (column 5, lines 55-65);

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client (column 5, lines 55-65 and column 6, lines 1-10).

59. Regarding claims 52, 86, 120 and 144, Candelore teaches sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form (column 5, lines 20-26 and column 6, lines 11-31 and 42-51);

wherein the access controlled data comprises the control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, and column 7, lines 25-41).

60. Regarding claims 53, 87 and 121, Candelore teaches descrambling media content using the control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41);

storing the media content in a storage under protection of a digital rights management system (column 6, lines 11-31 and 42-51).

61. Regarding claims 54, 88 and 122, Candelore teaches descrambling media content using the control word; and rendering the media content for presentation (column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

62. Regarding claims 55, 89 and 123, Candelore teaches retrieving the entitlement control message from a storage device (column 6, lines 11-31 and 42-51);
wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client (column 3, lines 61-67, column 4, lines 1-14 and 55-67 and column 5, lines 1-3 and 20-26).

63. Regarding claims 56, 90 and 124, Candelore teaches wherein the access controlled data comprises a decrypted version of the entitlement control message (column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

64. Regarding claims 60, 94 and 128, Candelore teaches wherein both the first and the second entitlement control messages contain a same control word (Figure 2, element 416 and Figure 3, elements 41, 44 and 45, column 3, lines 15-23, column 6,

lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41);

the second entitlement control message is encrypted to be decrypted using a key of the conditional access server (column 4, lines 6-14, column 6, lines 32-49 and column 7, lines 25-41).

65. Regarding claims 61, 95 and 129, Candelore teaches wherein the first entitlement control message contains a first control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 3, lines 15-24 and column 6, lines 14-17 and 60-63);

the second entitlement control message contains a second control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

the first and second control words are different (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

the access controlled data further comprises the first and second control words (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

the method further comprises: descrambling the content using the first control word and rescrambling the content using the second control word (column 5, lines 55-65).

66. Regarding claim 139, Candelore discloses a storage device coupled to the transcrambler, the storage device to store the content rescrambled by the second control word (column 5, lines 55-65).

67. Regarding claim 145, Candelore discloses a storage device;

a descrambler coupled to the processor and the storage device, the descrambler to descramble media content using the control word, the storage device to store the media content under protection of a digital rights management system (column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

Conclusion

68. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

69. The following United States Patents are cited to further show the state of the art with respect to the access control of content, such as:

United States Patent No. 7,127,619 to Unger et al., which is cited to show the decoding and decryption of partially encrypted information.

United States Patent No. 7,171,558 to Mourad et al., which is cited to show transparent digital rights management for extendible content viewers.

United States Patent No. 7,177,429 to Moskowitz et al., which is cited to show system and methods for permitting open access to data objects and for securing data within the data objects.

United States Patent No. 7,292,692 to Bonan et al., which is cited to show content scrambling with minimal impact on legacy devices.

United States Patent No. 7,316,032 to Tayebi et al., which is cited to show a method for allowing a customer to preview, acquire and/or pay for the information and a system therefor.

United States Patent No. 7,336,784 to Zuili which is cited to show a multimedia decoder method and system with authentication and enhanced digital rights management (DRM) where each received signal is unique and where the missing signal is cached inside the storage memory of each receiver.

70. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

71. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

72. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/

Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/007,116	Applicant(s)/Patent Under Reexamination VANTALON ET AL.	
	Examiner JEREMIAH AVERY	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,036,011	04-2006	Grimes et al.	713/156
*	B	US-7,127,619	10-2006	Unger et al.	713/193
*	C	US-7,171,558	01-2007	Mourad et al.	713/168
*	D	US-7,177,429	02-2007	Moskowitz et al.	380/252
*	E	US-7,292,692	11-2007	Bonan et al.	380/212
*	F	US-7,316,032	01-2008	Tayebi et al.	705/51
*	G	US-7,336,784	02-2008	Zuili, Patrick	380/200
*	H	US-7,302,058	11-2007	Candelore, Brant L.	380/200
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/27/2009	03/27/2009							
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓	O							
	25	✓	O							
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/27/2009	03/27/2009							
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	46	✓								
	47	✓								
	48	✓								
	49	✓								
	50	✓								
	51	✓								
	52	✓								
	53	✓								
	54	✓								
	55	✓								
	56	✓								
	57	✓								
	58	✓								
	59	✓								
	60	✓								
	61	✓								
	62	✓								
	63	✓								
	64	✓								
	65	✓								
	66	✓								
	67	✓								
	68	✓								
	69	✓								
	70	✓								
	71	✓								
	72	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/27/2009	03/27/2009							
	73	✓								
	74	✓								
	75	✓								
	76	✓								
	77	✓								
	78	✓								
	79	✓								
	80	✓								
	81	✓								
	82	✓								
	83	✓								
	84	✓								
	85	✓								
	86	✓								
	87	✓								
	88	✓								
	89	✓								
	90	✓								
	91	✓								
	92	✓								
	93	✓								
	94	✓								
	95	✓								
	96	✓								
	97	✓								
	98	✓								
	99	✓								
	100	✓								
	101	✓	O							
	102	✓								
	103	✓								
	104	✓								
	105	✓								
	106	✓								
	107	✓								
	108	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/27/2009	03/27/2009							
	109	✓								
	110	✓								
	111	✓								
	112	✓								
	113	✓								
	114	✓								
	115	✓								
	116	✓								
	117	✓								
	118	✓								
	119	✓								
	120	✓								
	121	✓								
	122	✓								
	123	✓								
	124	✓								
	125	✓								
	126	✓								
	127	✓								
	128	✓								
	129	✓								
	130	✓								
	131	✓								
	132	✓								
	133	✓								
	134	✓								
	135	✓								
	136	✓	O							
	137	✓								
	138	✓								
	139	✓								
	140	✓								
	141	✓								
	142	✓								
	143	✓								
	144	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/27/2009	03/27/2009							
	145	✓								
	146	✓	O							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

SEARCHED			
Class	Subclass	Date	Examiner
none	none	3/26/2009	JLA

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search	3/26/2009	JLA
Keywords in EAST Search	3/26/2009	JLA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
none	none	3/26/2009	JLA

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9254

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/007,116	12/07/2004	713	2431	6517P002

APPLICANTS

Luc Vantalon, Sunnyvale, CA;
Paolo Siccardo, Los Altos, CA;

** CONTINUING DATA **********

** FOREIGN APPLICATIONS **********

** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **
01/24/2005

Foreign Priority claimed ❑ Yes ☑ No 35 USC 119(a-d) conditions met ❑ Yes ☑ No Verified and Acknowledged /JEREMIAH L AVERY/ Examiner's Signature	❑ Met after Allowance JLA Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	19	146	15

ADDRESS

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040
UNITED STATES

TITLE

Methods and apparatuses for secondary conditional access server

FILING FEE RECEIVED		
4114	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

BIB (Rev. 05/07).

IPR2025-00305
ASUS EX1002 Page 332

OIPE
FEB 14 2005
JC37
PATENT & TRADEMARK OFFICE

FIW

Attorney Docket No. 06517.P002

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Luc Vantalon, et al

Application No.: 11/007,116

Filing Date: December 7, 2004

For: Methods and Apparatuses for Secondary Conditional Access Server

Examiner: Unknown
Art Unit: 2131

FIRST CLASS CERTIFICATE OF MAILING (37 C.F.R. § 1.8(a))
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

2-9-05
(Date of Deposit)

Joyce Klein
(Name of Person Mailing Correspondence)

(Signature) 2-9-05 (Date)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Examiner:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 together with copies of the documents cited on that form, except for copies not required to be submitted (e.g., copies of U.S. patents and U.S. published patent applications need not be enclosed). It is respectfully requested that the cited documents be considered and that the enclosed copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

IPR2025-00305
ASUS EX1002 Page 333

to be construed as an admission that the information cited in this statement is material to patentability.

Pursuant to 37 C.F.R. § 1.97, this Information Disclosure Statement is being submitted under one of the following (as indicated by an "X" to the left of the appropriate paragraph):

__x__ 37 C.F.R. §1.97(b).

_____ 37 C.F.R. §1.97(c). If so, then enclosed with this Information Disclosure Statement is one of the following:

____ A statement pursuant to 37 C.F.R. §1.97(e); or

____ A check for $180.00 for the fee under 37 C.F.R. § 1.17(p).

_____ 37 C.F.R. §1.97(d). If so, then enclosed with this Information Disclosure Statement are the following:

(1) A statement pursuant to 37 C.F.R. §1.97(e); and

(2) A check for $180.00 for the fee under 37 C.F.R. §1.17(p) for submission of the Information Disclosure Statement.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

Dated: 2/9, 2005

Lehua Wang
Reg. No. 48,023

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025-1026
(408) 720-8300

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

IPR2025-00305
ASUS EX1002 Page 334

Substitute for Form 1449A/PTO (Modified) (use as many sheets as necessary)	Attorney Docket No.: 6517.P002	Application Number: 11/007,116
	First Named Inventor: Luc Vantalon	
	Filing Date: 12/7/2004	

OIPE
FEB 14 2005
PATENT & TRADEMARK OFFICE
SC37

OTHER ART – NO PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	Translation[2]
		InterTrust's Right/System Platform. InterTrust Technologies Corp.	
		Conditional Access (CA) Tutorial. Digital TV Group. www.dtg.org.uk/reference/tutorial/ca.htm. August 2004. 2 pages.	
		RENATO IANNELLA. "Digital Rights Management (DRM) Architectures". D-Lib Magazine, June 2001. Volume 7, Number 6. ISSN 1082-9873. Pages 1-10.	
		MARK MASSEL. "Conditional Access". Broadcasting Engineering, October 2001.	
		ATSC Standard: Conditional Access System for Terrestrial Broadcast, Revision A. Advanced Television Systems Committee, July 2004. Pages 1-31.	

Examiner Signature	/Jeremiah Avery/	Date Considered	03/23/2009

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication.

[1]Unique citation designation number. [2]Applicant is to place a check mark here if English language Translation is attached.

0651AP002REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

IPR2025-00305
ASUS EX1002 Page 335

OIPE JC37
FEB 14 2005
PATENT & TRADEMARK OFFICE

TRANSMITTAL **PATENT**

Application No.: 10/007,116
Filing Date: December 7, 2004
First Named Inventor: Luc Vantalon
Examiner's Name: ~~Unknown~~ J. Avery
Art Unit: ~~2131~~ 2431
Attorney Docket No.: 06517.P002

____ An Amendment After Final Action (37 CFR 1.116) is attached and applicant(s) request expedited action.
__X__ Charge any fee not covered by any check submitted to Deposit Account No. 02-2666.
__X__ Applicant(s) hereby request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 CFR 1.16 and 1.17, for any concurrent or future reply to Deposit Account No. 02-2666.
____ Applicant(s) claim small entity status (37 CFR 1.27).

ATTACHMENTS

____ Preliminary Amendment
____ Amendment/Response with respect to Office Action
____ Amendment/Response After Final Action (37 CFR 1.116) (reminder: consider filing a Notice of Appeal)
____ Notice of Appeal
____ RCE (Request for Continued Examination)
____ Supplemental Declaration
____ Terminal Disclaimer (reminder: if executed by an attorney, the attorney must be properly of record)
__X__ Information Disclosure Statement (IDS)
__X__ Copies of IDS citations
____ Petition for Extension of Time
____ Fee Transmittal Document (that includes a fee calculation based on the type and number of claims)
____ Cross-Reference to Related Application(s)
____ Certified Copy of Priority Document
____ Other: _____
____ Other: _____
____ Check(s)
__X__ Postcard (Return Receipt)

SUBMITTED BY:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
TYPED OR PRINTED NAME: Lehua Wang
SIGNATURE:. Lehua Wang
REG. NO.: 48,023
DATE: 2/9/2005
ADDRESS: 12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025
TELEPHONE NO.: (408) 720-8300

CERTIFICATE OF MAILING BY FIRST CLASS MAIL (if applicable)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria Virginia 22313-1450 on

2-9-05
Date of Deposit

Joyce Klein
Name of Person Mailing Correspondence

Signature

2-9-05
Date

(10/14/03)

Send to: COMMISSIONER FOR PATENTS, P.O. Box 1450, Alexandria, Virginia 22313-1450

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

IPR2025-00305
ASUS EX1002 Page 336

OIPE
MAY 03 2006
PATENT & TRADEMARK OFFICE
IAP100

Atty. Docket No. 006517.P002 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Luc Vantalon, *et al.*

Application No. 11/007,116

Filed: December 7, 2004

For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

Examiner: Not yet assigned.

Art Unit: 2131

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

INFORMATION DISCLOSURE STATEMENT

Sir:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 together with copies of the documents cited on that form, except for copies not required to be submitted (e.g., copies of U.S. patents and U.S. published patent applications need not be enclosed). It is respectfully requested that the cited documents be considered and that the enclosed copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Pursuant to 37 C.F.R. § 1.97, this Information Disclosure Statement is being submitted under one of the following (as indicated by an "X" to the left of the appropriate paragraph):

_____ 37 C.F.R. §1.97(b).

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

IPR2025-00305
ASUS EX1002 Page 337

__X__ 37 C.F.R. §1.97(c). If so, then enclosed with this Information Disclosure Statement is one of the following:

__X__ A statement pursuant to 37 C.F.R. §1.97(e) or

____ A check for $_____ for the fee under 37 C.F.R. § 1.17(p).

_____ 37 C.F.R. §1.97(d). If so, then enclosed with this Information Disclosure Statement are the following:

(1) A statement pursuant to 37 C.F.R. §1.97(e); and

(2) A check for $_____ for the fee under 37 C.F.R. §1.17(p) for submission of the Information Disclosure Statement.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 5/1, 2006

James C. Scheller, Jr.
Reg. No. 31,195

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8300

FIRST CLASS CERTIFICATE OF MAILING (37 C.F.R. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on: May 1, 2006.

Date of Deposit

Cathi L.G. Thoorsell

Name of Person Mailing Correspondence

Cathi L.G. Thoorsell — Signature

May 1, 2006 — Date

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

IPR2025-00305
ASUS EX1002 Page 338

Substitute for Form 1449/PTO			Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*			Application Number	11/007,116
			Filing Date	December 7, 2004
			First Named Inventor:	Luc Vantalon
			Art Unit	~~2131~~ 2431
			Examiner Name	J. Avery
Sheet 1	of	2	Attorney Docket No.	006517.P002

OIPE MAY 0 3 2006 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Exmnr Initials*	Cite No.[1]	Document Number: Number	Document Number: Kind Code[2] (If known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US-2003/196092	A1	10-16-2003	Raley, M., *et al.*	

FOREIGN PATENT DOCUMENTS

Exmnr Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	2	FR 2 843 257 A1	02-06-2004	Viaccess		
	3	WO 03/010722 A2	02-06-2003	SCM Microsystems GMBH		
	4	EP 0 858 184 A2	08-12-1998	NDS Limited		
	5	WO 00/56068 A1	09-21-2000	Thomson Licensing S.A.		
	6	EP 0 691 787 A1	01-10-1996	Sony Corporation		

Examiner Signature	/Jeremiah Avery/	Date Considered	03/23/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.
If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08A (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

Substitute for Form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	11/007,116
				Filing Date	December 7, 2004
				First Named Inventor:	Luc Vantalon
				Art Unit	~~2131~~ 2431
				Examiner Name	Jeremiah Avery
Sheet	2	**of**	2	Attorney Docket No.	006517.P002

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	7	VAN MOFFAERT, A., *et al.,* "Digital Rights Management: DRM is a key enabler for the future growth of the broadband access market, and the telecom/networking market in general." Alcatel Telecommunications Review, Alcatel, Paris Cedex, FR, April 2003 (2003-2004), XP007005930 ISSN: 1267-7167, pages 1-7.	
	8	International Search Report and Written Opinion of the International Searching Authority for PCT/US2005/039794, mailed April 3, 2006, 11 pages.	

Examiner Signature	/Jeremiah Avery/	Date Considered	03/23/2009

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08B (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 08/10/03.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

IPR2025-00305
ASUS EX1002 Page 340

OIPE
MAY 03 2006
PATENT & TRADEMARK OFFICE

Atty. Docket No. 006517.P002

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Application of:

Luc Vantalon, *et al.*

Application No. 11/007,116

Filed: December 7, 2004

For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

Examiner: Not yet assigned.

Art Unit: 2131

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, PO Box 1450, Alexandria, Virginia 22313-1450

on 05-01-2006
Date of Deposit

Cathi L. G. Thoorsell
Name of Person Mailing Correspondence

Cathi L. G. Thoorsell May 1, 2006
Signature Date

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

STATEMENT UNDER 37 C.F.R. §1.97(e)

Sir:

I hereby certify (as indicated by an "X" to the left of the appropriate paragraph):

X That each item of information contained in the accompanying Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement.

____ That no item of information contained in the accompanying Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned attorney after making reasonable inquiry, no item of information contained in the Information Disclosure Statement was known to any individual designated in §1.56(c) more than three months prior to the filing the Information Disclosure Statement.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 5/1, 2006

James C. Scheller, Jr.
Reg. No. 31,195

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8300

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

IPR2025-00305
ASUS EX1002 Page 341

Substitute for Form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	11/007,116
				Filing Date	December 7, 2004
				First Named Inventor:	Luc Vantalon, et al.
				Art Unit	~~4192~~ 2431
				Examiner Name	~~Brian E. Weinrich~~ J. Avery
Sheet	1	**of**	1	Attorney Docket Number	6517.P002

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	1	PCT Notification Concerning Transmittal of Copy of International Preliminary report on Patentability, Date June 21, 2007, 7 Pages.	

Examiner Signature	/Jeremiah Avery/	Date Considered	03/23/2009

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	990	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT	OR	ON	2009/03/26 19:43
L2	873	l1 and server	US-PGPUB; USPAT	OR	ON	2009/03/26 19:48
L3	522	l2 and unauthori$	US-PGPUB; USPAT	OR	ON	2009/03/26 19:49
L4	447	l3 and (authoris$ or authoriz$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:49
L5	433	l4 and (ID or identit$ or identif$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:50
L6	420	l5 and ((first or primary) or (second$ or other) near server)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:50
L7	402	l6 and (broadcast$ or transmit$ or transmission or send$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:52
L8	395	l7 and ((broadcast$ or transmit$ or transmission or send$) same (media or audio or video or stream or content or data or information))	US-PGPUB; USPAT	OR	ON	2009/03/26 19:52
L9	317	l8 and (play$ or playback)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:53
L10	150	l9 and (subscribe$ or subscript$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:54
L11	39	l10 and $2scrambl$	US-PGPUB; USPAT	OR	ON	2009/03/26 19:54
L12	7	l11 and (control$5 near word)	US-PGPUB; USPAT	OR	ON	2009/03/26 20:00

3/ 26/ 2009 8:11:41 PM

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	)	
	)	Examiner: Avery, Jeremiah L.
Luc Vantalon	)	
	)	Art Unit: 2431
Application No: 11/007,116	)	
	)	
Filed: December 7, 2004	)	Confirmation No.: 9254
	)	
For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	)	

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

Dear Sir:

In response to the Office Action dated April 1, 2009, Applicant respectfully requests that the above-identified application be amended as follows and that the following remarks be considered:

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

June 12, 2009
Date of Deposit

Cynthia Mirelez
Name of Person Filing Correspondence

Signature

June 12, 2009
Date

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method to control a presentation of content, the method comprising:

receiving a representation of content from a first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access; and

presenting the content, at a user's request, through a second conditional access server which is coupled to the first conditional access server;

wherein the presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively; ~~and~~

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content; and

wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process and the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process.

2. (Original) The method of claim 1, wherein the content is presented by a network client of the second conditional access server using the second set of cryptographic keys.

3. (Original) The method of claim 2, wherein the first conditional access server provides the second conditional access server the first set of cryptographic keys for authorized use.

4. (Original) The method of claim 3, wherein the user's request is after the first conditional access server provides at least a portion of the content; and the portion of the content is presented in response to the user's request.

5. (Original) The method of claim 2, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the network client is a digital rights management client.

6. (Original) The method of claim 5, wherein the second conditional access server authorizes the network client to use the content through the digital rights management system in accordance with authorization to use received from the first conditional access server.

7. (Original) The method of claim 1, wherein the second conditional access server translates authorization to access the content from authorization received from the first conditional access server to authorization for the network client.

8. (Original) The method of claim 1, wherein the second set of cryptographic keys consists one key.

9. (Original) The method of claim 1, wherein the second conditional access server acts as a primary conditional access server to another secondary conditional access server.

10. (Currently Amended) A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content, the method comprising:

receiving, at a second conditional access server, a first set of cryptographic keys from a first conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys; and

authorizing a client of the second conditional access server to present the content in accordance with authorization the second conditional access server received from the first conditional access server;

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content; and

wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process and the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process.

11. (Original) The medium of claim 10, wherein the method further comprises:

recording a representation of the content in an encrypted form in response to a message from the first conditional access server.

12. (Original) The medium of claim 11, wherein the client sends a request, through a network connection to the second conditional access server, for authorization to present the content after the first conditional access server provides at least a portion of the content which is recorded; and the second conditional access server obtains authorization from the first conditional access server, after the first conditional access server provides the portion of the content, for said authorizing.

13. (Original) The medium of claim 10, wherein the method further comprises:

translating authorization to access the content from authorization received from the first conditional access server to authorization for the client.

14. (Original) The medium of claim 13, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the client comprises a digital rights management client.

15. (Original) The medium of claim 14, wherein the second conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the first conditional access server.

16. (Original) The medium of claim 15, wherein the first conditional access server provides authorization to the second conditional access server according to an identity of the second conditional access server; the second conditional access server provides authorization to the client according to an identity of the client; and the first conditional access server is not aware of an identity of the client.

17. (Original) The medium of claim 10, wherein the second set of cryptographic keys consists one key.

18. (Original) The medium of claim 10, wherein the second conditional access server is a server of a further secondary conditional access server and acts as a primary conditional access server with respect to the further secondary conditional access server.

19. (Currently Amended) A secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

a communication interface, the communication interface to receive a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys; and

a controller coupled to the communication interface, the controller to authorize a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server;

wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content, and

wherein the primary conditional access server authenticates clients of the primary conditional access server through a first authentication process and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process.

20. (Original) The secondary conditional access server of claim 19, wherein the controller is to translate authorization to access the content from authorization received from the primary conditional access server to authorization for the client.

21. (Original) The secondary conditional access server of claim 20, wherein the second set of cryptographic keys comprises a key of a digital rights management system; the client comprises a digital rights management client; and the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server.

22. (Original) The secondary conditional access server of claim 20, wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary

conditional access server provides authorization to the client according to an identity of the client; and the primary conditional access server is not aware of an identity of the client.

23. (Currently Amended) A secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

means for receiving a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys; and

means for authorizing a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server;

wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content, and

wherein the primary conditional access server authenticates clients of the primary conditional access server through a first authentication process and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process.

24. (Currently amended) The secondary conditional access server of claim 23, further comprising:

means for recording a representation of the content in an encrypted form in response to a message from the primary conditional access server[[.]].

wherein the client sends a request, through a network connection to the secondary conditional access server, for authorization to present the content after the primary conditional access server provides at least a portion of the content which is recorded; and

the secondary conditional access server obtains authorization from the primary conditional access server, after the primary conditional access server provides the portion of the content, for authorizing the client to present the content.

25. (Currently amended) The secondary conditional access server of claim 23, further comprising:

means for translating authorization to access the content from authorization received from the primary conditional access server to authorization for the client[[.]],

wherein the second set of cryptographic keys comprises a key of a digital rights management system; and

the client comprises a digital rights management client; and

wherein the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server.

26. (Original) The secondary conditional access server of claim 23, wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of the client; and the primary conditional access server is not aware of an identity of the client.

27. (Original) The secondary conditional access server of claim 23, wherein the second set of cryptographic keys consists one key.

28. (Currently Amended) A method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component;

broadcasting the media component from a first conditional access server;

receiving a client request to use the media component from a client through a second conditional access server after said broadcasting; and

responding to the client request through the second conditional access server,

wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process and the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process.

29. (Original) The method of claim 28, further comprising:

broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

30. (Original) The method of claim 29, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

31. (Original) The method of claim 30, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

32. (Currently Amended) A method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system;

processing the security messages on the conditional access server; and

transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process.

33. (Original) The method of claim 32, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system.

34. (Original) The method of claim 32, wherein the access controlled data is protected using a digital rights management system.

35. (Original) The method of claim 34, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

36. (Original) The method of claim 34, further comprising:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

37. (Original) The method of claim 36, wherein the access controlled data comprises a decrypted version of the entitlement control message.

38. (Original) The method of claim 34, further comprising:

receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

39. (Original) The method of claim 38, further comprising:

storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

40. (Original) The method of claim 32, further comprising:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

41. (Original) The method of claim 40, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

42. (Original) The method of claim 41, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

43. (Original) The method of claim 41, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

44. (Original) The method of claim 41, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

45. (Original) The method of claim 44, wherein the access controlled data further comprises the first and second control words.

46. (Original) The method of claim 32, further comprising:

receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

generating a second entitlement control message containing a second control word that is different from the first control word; and

descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

47. (Original) The method of claim 46, further comprising:

storing, at the conditional access server, the content rescrambled by the second control word; and

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

48. (Currently amended) A method to process media content provided by a primary security system, the method comprising:

receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system,

wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process.

49. (Original) The method of claim 48, wherein the security message is an entitlement message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

50. (Original) The method of claim 48, wherein the access controlled format protects access to data using a digital rights management system.

51. (Original) The method of claim 50, further comprising:

automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

descrambling and recording the portion of the media content in response to a determination to descramble; and

recording the portion of the media content without descrambling in response to a determination not to descramble.

52. (Original) The method of claim 50, further comprising:

sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

53. (Original) The method of claim 52, further comprising:

descrambling media content using the control word; and

storing the media content in a storage under protection of a digital rights management system.

54. (Original) The method of claim 52, further comprising:

descrambling media content using the control word; and

rendering the media content for presentation.

55. (Original) The method of claim 54, further comprising:

retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second

entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

56. (Original) The method of claim 52, wherein the access controlled data comprises a decrypted version of the entitlement control message.

57. (Original) The method of claim 50, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

58. (Original) The method of claim 48, further comprising:

receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

59. (Original) The method of claim 58, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the method further comprises:

storing the second entitlement control message with the portion of the media content.

60. (Original) The method of claim 59, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

61. (Original) The method of claim 59, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control

word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further comprises:

descrambling the content using the first control word and rescrambling the content using the second control word.

62. (Currently Amended) A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component;

broadcasting the media component from a first conditional access server;

receiving a client request to use the media component from a client through a second conditional access server after said broadcasting; and

responding to the client request through the second conditional access server, wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process and the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process.

63. (Original) The medium of claim 62, wherein the method further comprises:

broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

64. (Original) The medium of claim 63, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

65. (Original) The medium of claim 64, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

66. (Currently amended) A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system;

processing the security messages on the conditional access server; and

transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process.

67. (Original) The medium of claim 66, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system.

68. (Original) The medium of claim 66, wherein the access controlled data is protected using a digital rights management system.

69. (Original) The medium of claim 68, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

70. (Original) The medium of claim 68, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

71. (Original) The medium of claim 70, wherein the access controlled data comprises a decrypted version of the entitlement control message.

72. (Original) The medium of claim 68, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

73. (Original) The medium of claim 72, wherein the method further comprises:

storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

74. (Original) The medium of claim 66, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

75. (Original) The medium of claim 74, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

76. (Original) The medium of claim 75, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

77. (Original) The medium of claim 75, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

78. (Original) The medium of claim 75, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

79. (Original) The medium of claim 78, wherein the access controlled data further comprises the first and second control words.

80. (Original) The medium of claim 66, wherein the method further comprises:

receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

generating a second entitlement control message containing a second control word that is different from the first control word; and

descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

81. (Original) The medium of claim 80, wherein the method further comprises:

storing, at the conditional access server, the content rescrambled by the second control word; and

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

82. (Currently amended) A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process media content provided by a primary security system, the method comprising:

receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system,

wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process.

83. (Original) The medium of claim 82, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

84. (Original) The medium of claim 82, wherein the access controlled format protects access to data using a digital rights management system.

85. (Original) The medium of claim 84, wherein the method further comprises:

automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

descrambling and recording the portion of the media content in response to a determination to descramble; and

recording the portion of the media content without descrambling in response to a determination not to descramble.

86. (Original) The medium of claim 84, wherein the method further comprises:

sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

87. (Original) The medium of claim 86, wherein the method further comprises:

descrambling media content using the control word; and

storing the media content in a storage under protection of a digital rights management system.

88. (Original) The medium of claim 86, wherein the method further comprises:

descrambling media content using the control word; and

rendering the media content for presentation.

89. (Original) The medium of claim 88, wherein the method further comprises:

retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

90. (Original) The medium of claim 86, wherein the access controlled data comprises a decrypted version of the entitlement control message.

91. (Original) The medium of claim 84, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

92. (Original) The medium of claim 82, wherein the method further comprises:

receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

93. (Original) The medium of claim 92, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the method further comprises:

storing the second entitlement control message with the portion of the media content.

94. (Original) The medium of claim 93, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

95. (Original) The medium of claim 93, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further comprises:

descrambling the content using the first control word and rescrambling the content using the second control word.

96. (Currently Amended) A primary security system to provide conditional access, the system comprising:

means for broadcasting a first entitlement management message for a subscriber to request caching of a media component;

means for broadcasting the media component;

means for receiving a client request to use the media component from a client through a secondary conditional access server after said broadcasting; and

means for responding to the client request through the secondary conditional access server,

wherein the primary security system authenticates clients of the primary security system through a first authentication process and the secondary conditional access server authenticates clients of the secondary conditional access server through a

EX1002 - Page 367
IPR2025-00305
ASUS EX1002 Page 367

second authentication process which is independent of the first authentication process.

97. (Original) The system of claim 96, further comprising:

means for broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

98. (Original) The system of claim 97, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

99. (Original) The system of claim 98, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

100. (Currently amended) A data processing system to process conditional access protection, the data processing system comprising:

means for receiving, at a conditional access server, security messages of a primary security system;

means for processing the security messages on the conditional access server; and

means for transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server

authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process.

101. (Currently amended) The data processing system of claim 100, wherein the security messages comprise entitlement management [[messags]] messages; the conditional access server has a user key representing a subscriber of the primary security system; and said means for processing the entitlement management messages comprises:

means for decrypting to obtain a service key of the primary security system.

102. (Original)The data processing system of claim 100, wherein the access controlled data is protected using a digital rights management system.

103. (Original)The data processing system of claim 102, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

104. (Original)The data processing system of claim 102, further comprising:

means for receiving, at the conditional access server, an entitlement control message of the primary security system; and

means for processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

105. (Original)The data processing system of claim 104, wherein the access controlled data comprises a decrypted version of the entitlement control message.

106. (Original)The data processing system of claim 102, further comprising:

means for receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

means for descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

107. (Original)The data processing system of claim 106, further comprising:

means for storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

108. (Original)The data processing system of claim 100, further comprising:

means for receiving, at the conditional access server, an entitlement control message of the primary security system; and

means for processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

109. (Original)The data processing system of claim 108, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

110. (Original)The data processing system of claim 109, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

111. (Original)The data processing system of claim 109, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

112. (Original)The data processing system of claim 109, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

113. (Original)The data processing system of claim 112, wherein the access controlled data further comprises the first and second control words.

114. (Original)The data processing system of claim 100, further comprising:

means for receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

means for generating a second entitlement control message containing a second control word that is different from the first control word; and

means for descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

115. (Original)The data processing system of claim 114, further comprising:

means for storing, at the conditional access server, the content rescrambled by the second control word; and

means for retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

116. (Currently amended) A data processing system to process media content provided by a primary security system, the data processing system comprising:

means for receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system,

wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process.

117. (Original)The data processing system of claim 116, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

118. (Original)The data processing system of claim 116, wherein the access controlled format protects access to data using a digital rights management system.

119. (Original)The data processing system of claim 118, further comprising:

means for automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

means for descrambling and recording the portion of the media content in response to a determination to descramble; and

means for recording the portion of the media content without descrambling in response to a determination not to descramble.

120. (Original)The data processing system of claim 118, further comprising:

means for sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

121. (Original)The data processing system of claim 120, further comprising:

means for descrambling media content using the control word; and

means for storing the media content in a storage under protection of a digital rights management system.

122. (Original)The data processing system of claim 120, further comprising:

means for descrambling media content using the control word; and

means for rendering the media content for presentation.

123. (Original)The data processing system of claim 122, further comprising:

means for retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

124. (Original)The data processing system of claim 120, wherein the access controlled data comprises a decrypted version of the entitlement control message.

125. (Original)The data processing system of claim 118, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

126. (Original)The data processing system of claim 116, further comprising:

means for receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

means for sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

127. (Original)The data processing system of claim 126, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the system further comprises:

means for storing the second entitlement control message with the portion of the media content.

128. (Original)The data processing system of claim 127, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

129. (Original)The data processing system of claim 127, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the system further comprises:

means for descrambling the content using the first control word and rescrambling the content using the second control word.

130. (Currently amended) A conditional access server, comprising:

one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system;

a processor coupled to the one or more communication interfaces, the processor to process the security messages, and the one or more communication interfaces to transmit, to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process.

131. (Original)The conditional access server of claim 130, wherein the security messages comprise entitlement management messages; and the access controlled data is protected using a digital rights management system.

132. (Original)The conditional access server of claim 131, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

133. (Original)The conditional access server of claim 131, wherein the one or more communication interfaces are to receive an entitlement control message of the primary security system; the processor is to obtain a control word of the primary security system

from the entitlement control message; and the access controlled data comprises the control word.

134. (Original)The conditional access server of claim 131, wherein the one or more communication interfaces are to receive an entitlement control message and scrambled content of the primary security system; and the conditional access server further comprises:

a descrambler coupled to the processor, the descrambler to descramble the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

135. (Original)The conditional access server of claim 134, further comprising:

a storage device coupled to one or more communication interfaces, the storage device to store the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

136. (Currently amended) The conditional access server of claim 130, wherein the one or more communication interfaces are to receive entitlement control message of the primary security system; the processor is to [[to]] generate a substitutive entitlement control message as a replacement of the entitlement control message; and the access controlled data comprises the substitutive entitlement control message.

137. (Original)The conditional access server of claim 136, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

138. (Original)The conditional access server of claim 130, wherein the one or more communication interfaces are to receive a first entitlement control message containing a first control word and content scrambled by the first control word; the processor is to generate a second entitlement control message containing a second control word that is different from the first control word; and the conditional access server further comprises:

a transcrambler coupled to the one or more communication interfaces and the processor, the transcrambler to descramble the content using the first control word and rescramble the content using the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

139. (Original)The conditional access server of claim 138, further comprising:

a storage device coupled to the transcrambler, the storage device to store the content rescrambled by the second control word.

140. (Currently amended) A secondary conditional access client, comprising:

a communication interface to receive, from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system; and

a processor coupled to the communication interface, the processor to process the access controlled data,

wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server

authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process.

141. (Original)The client of claim 140, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

142. (Original)The client of claim 140, wherein the access controlled format protects access to data using a digital rights management system.

143. (Original)The client of claim 142, wherein the processor is to automatically determine whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data; the client further comprises:

a storage device;

a descrambler coupled to the processor and the storage device, in response to a determination to descramble the descrambler to descramble the portion of the media content for storing in the storage device, in response to a determination not to descramble the storage device to record the portion of the media content without descrambling.

144. (Original)The client of claim 142, wherein the communication interface is to send, to the conditional access server through a network connection, an entitlement control message containing a control word in an encrypted form; and the access controlled data comprises the control word.

145. (Original)The client of claim 144, further comprising:

a storage device;

a descrambler coupled to the processor and the storage device, the descrambler to descramble media content using the control word, the storage device to store the media content under protection of a digital rights management system.

146. (Currently Amended) The client of claim 140, further comprising:

[[an]]a physical interface to receive a first entitlement control message for descrambling a portion of media content received from the primary security system; and

wherein the communication interface is to send the first entitlement control message to the conditional access server through a network connection.

REMARKS

Claim Objections

The Examiner has objected to claims 24, 25, 101, 136 and 146 because of informalities. Applicant has amended the claims to correct the informalities.

35 U.S.C. § 103 Rejections

The Examiner has rejected claims 1-35, 37-40, 48-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132, 134-136, 137, 140-143 and 146 under 35 U.S.C. § 102(e) as being anticipated by Grimes (U. S. Patent No. 7,036,011).

Applicant has amended the claims to particularly point out the innovative features of the present invention. Specifically, applicant has added a limitation that the first/second CA server authenticates its clients through a first/second authentication process respectively, and the first and second authentication processes are independent of each other. Applicant submits that there is no new material added, and that support for the present amendment can be found at least in paragraph [0057].

Applicant submits that the present invention is not anticipated by Grimes, since Grimes fails to disclose or teach at least an element of the present claims, namely two independent authentication processes from two CA servers.

In an embodiment, the present invention provides bridging between two security systems so that a secondary security system can securely present to a user a content previously secured by a primary security system. The present bridging process connects two independent authentication processes through a relationship between the two security systems.

For example, the primary security system can be a first conditional access (CA) server, servicing clients of the first CA server using a first authentication process. The secondary security system can be a second CA server, servicing clients of the second CA server using a second authentication process, which is independent of the first authentication process. The present invention provides a bridging service between a first CA client and a second CA server, allowing the second CA server to receive content after being authenticated by the first CA server, and to present the content to a user pending a successful second authentication process.

In the prior art approaches, a client of a secondary CA server would need to subscribe to the primary CA server in order to receive services from the primary CA server. An advantage of the present bridging service allows a user to receive secured content from a primary system without directly subscribing to the primary system services. The service from the primary system can be received by the secondary system, which then presents it to the user.

Applicant submits that Grimes discloses a mechanism for providing secure access of protected content to users, employing a standalone digital certificate (Col. 1, lines 55-67). After receiving an encrypted content with a digital certificate, a user then sends the digital certificate to request the encryption key for descrambling the encrypted content. Thus Grimes discloses two separate but related steps in securing the protection of encrypted content: sending a digital certificate to the user, and requiring the user to use the digital certificate to exchange for the encryption key. While the system sending the encrypted content can be separate from the system to send the encryption key, there is only one authentication process for the user.

Applicant submits that Grimes fails to teach or disclose two security systems having two independent authentication processes. The two independent authentication processes are bridged

through a client server relationship between the two security systems to allow the second security system to present to a user the encrypted content of the first security system.

In addition, applicant submits that Grimes also fails to teach other elements of the present invention, for example, first and second sets of cryptographic keys to protect the content (independent claims 1, 10, 19, and 23); and access controlled data of a second CA server that is partially derived from a first CA server (independent claims 32, 66, 100, 130, and 48, 82, 116).

Applicant submits that Grimes only discloses one set of cryptographic key to protect the content. Grimes also discloses a method to uniquely identify the cryptographic key that has been used to encrypt the received content by requiring the use of a digital certificate. Applicant submits that the digital certificate does not protect the content, but is an extra safeguard for the authentication of the encrypted content.

Applicant further submits that Grimes does not disclose that the access controlled data of a second CA server can be partially derived from the security message of the first CA server. The present invention discloses, in an embodiment, a bridging service between two independent authentication processes with the access controlled data from the second CA server, in an embodiment, are partially derived from the security message of the first CA server.

In contrast, Grimes only discloses a process of sending a digital certificate in exchange for an encryption key. The encryption key (e.g., the access controlled data from the DRM server) is different and not part of the digital certificate (e.g., a security message from a content server).

Applicant, accordingly, respectfully requests withdrawal of the rejection of claims 1-35, 37-40, 48-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132, 134-136, 137, 140-143 and 146 under 35 U.S.C. § 102(e) as being anticipated by Grimes.

35 U.S.C. § 103 Rejections

The Examiner has rejected claims 36, 41-17, 52-56, 60, 61, 70, 75-81, 86-90, 94, 95, 104, 109-115, 120-124, 128, 129, 133, 137-139, 144 and 145 under 35 U.S.C. § 103(a) as being unpatentable over Grimes as applied to claims 32, 66, 100, 130 and 140 above, and further in view of Candelore (U. S. Patent No. 7,302,058). Candelore fails to disclose the limitations noted above and hence does not cure the deficiencies in Grimes.

Applicant submits that these claims are dependent claims, thus should be allowable, at least for the reasons stated above.

CONCLUSION

Applicant respectfully submits that the present application is in condition for allowance.

If there are any additional charges, please charge them to our Deposit Account No. 02-2666. If a telephone conference would facilitate the prosecution of this application, the Examiner is invited to contact the undersigned at (408) 720-8300.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: June 12, 2009

James C. Scheller, Jr.
Reg. No. 31,195

Customer No. 008791
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

Electronic Acknowledgement Receipt

EFS ID:	5510794
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	08791
Filer:	James Scheller Jr./Cynthia Mirelez
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	6517P002
Receipt Date:	12-JUN-2009
Filing Date:	07-DEC-2004
Time Stamp:	18:56:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		6517P002_RESPONSE.pdf	1415119 bddc9fa1d8449b0ed3f6cf9660c3162d1e4d6c23	yes	40

IPR2025-00305
ASUS EX1002 Page 385

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	35
	Applicant Arguments/Remarks Made in an Amendment	36	40
Warnings:			
Information:			
	Total Files Size (in bytes):	1415119	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IPR2025-00305
ASUS EX1002 Page 386

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/007,116	12/07/2004	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	06/12/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 146	Minus	** 146	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 15	Minus	***15	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/BRUCE D. HARRISON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

8791 7590 12/08/2009

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/007,116	VANTALON ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-146* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-146* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

I. Claims 1-146 have been examined.

II. Responses to Applicant's Remarks have been given.

Response to Arguments

1. Applicant's arguments, see page 36, filed 6/12/09, with respect to the objections to claims 24, 25, 101, 136 and 146 have been fully considered and are persuasive. The objections to claims 24, 25, 101, 136 and 146 have been withdrawn.

2. Further, the Applicant's arguments that pertain to the newly added claim language are rendered moot in view of the new grounds of rejection set forth below.

3. The Applicant argues that "Grimes fails to teach or disclose two security systems having two independent authentication processes". With the generation of identification(s) and each one being authenticated at the separate first and second systems (e.g. "the validity of the one or more second child vouchers is authenticated by the second parent client"), the Examiner asserts that the utilization of the Simelius reference teaches this aspect of the claimed invention, as cited below.

4. Further, the Applicant argues that within Grimes, "the digital certificate does not protect the content, but is an extra safeguard for the authentication of the encrypted content". The Examiner asserts that a safeguard is a means of protection.

5. With regards to the Applicant's argument that "Candelore fails to disclose the limitations noted above and hence does not cure the deficiencies in Grimes", the Examiner asserts that Candelore significantly discloses the parts of the claimed invention pertaining to the "control words", as cited below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-35, 37-40, 4-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132, 134-136, 137, 140-143 and 146 are rejected under 35 U.S.C. 103(a) as being unpatentable over by United States Patent No. 7,036,011 to Grimes et al., hereinafter Grimes, and further in view of United States Patent No. 7,493,291 to Simelius, hereinafter Simelius.

6. Regarding claim 1, Grimes teaches a method to control a presentation of content, the method comprising:

receiving a representation of content from a first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access (column 2, lines 1-31, “content is encrypted with an encryption key”);

IPR2025-00305
ASUS EX1002 Page 391

presenting the content, at a user's request, through a second conditional access server which is coupled to the first conditional access server (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

wherein the presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”);

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content (column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

7. Grimes significantly teaches the claimed invention, as cited above. However, Grimes does not substantially teach the claim language with regards to “wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process and the second conditional access server authenticates clients of the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process”. Simelius teaches said claim language, as cited below.

8. Regarding claim 1, Simelius teaches wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process and the second conditional access server authenticates clients of the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

9. The motivation to combine would be “This provides a solution for more flexible use of digital content across a plurality of devices, while the use cannot be freely copied.” (*Simelius* – column 7, lines 63-65).

10. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Simelius with the teachings of Grimes so that “the exchange of rights to access digital content between devices will facilitate a user-friendly environment in any situation for consuming the digital content” (*Simelius* – column 7, lines 65-67).

11. Further, the claim language within claims 10, 28 and 62 is analogous to the claim language set forth within claim 1, thus the motivation and obviousness to combine for claim 1 will also pertain to claims 10, 28 and 62.

12. Regarding claim 2, Grimes teaches wherein the content is presented by a network client of the second conditional access server using the second set of

cryptographic keys (column 4, lines 20-28, column 5, lines 50-56, column 6, lines 35-52, “encrypting and transmitting the encryption key 98” and column 7, lines 30-51).

13. Regarding claim 3, Grimes teaches wherein the first conditional access server provides the second conditional access server the first set of cryptographic keys for authorized use (column 5, lines 50-56, column 6, lines 35-52, column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62 and column 9, lines 38-60).

14. Regarding claim 4, Grimes teaches wherein the user's request is after the first conditional access server provides at least a portion of the content; and the portion of the content is presented in response to the user's request (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

15. Regarding claims 5 and 14, Grimes teaches wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the network client is a digital rights management client (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

16. Regarding claims 6 and 14, Grimes teaches wherein the second conditional access server authorizes the network client to use the content through the digital rights

management system in accordance with authorization to use received from the first conditional access server (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

17. Regarding claims 7 and 20, Grimes teaches wherein the second conditional access server translates authorization to access the content from authorization received from the first conditional access server to authorization for the network client (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

18. Regarding claims 8, 17 and 27, Grimes teaches wherein the second set of cryptographic keys consists one key (column 2, lines 1-31, “content is encrypted with an encryption key”).

19. Regarding claim 9, Grimes teaches wherein the second conditional access server acts as a primary conditional access server to another secondary conditional access server (column 7, lines 18-23, “the DRM server 58 or other server at the NOC 12”, column 8, lines 16-31, “third-party website server” and column 9, lines 3-11).

20. Regarding claim 10, Grimes discloses a machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content, the method comprising:

receiving, at a second conditional access server, a first set of cryptographic keys from a first conditional access server which provides a representation of content in an

encrypted form and authorizes access to the content through the first set of cryptographic keys (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

authorizing a client of the second conditional access server to present the content in accordance with authorization the second conditional access server received from the first conditional access server (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”);

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content (column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

21. Regarding claim 10, Simelius discloses wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process and the second conditional access server authenticates clients of the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-

4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

22. Regarding claim 11, Grimes discloses wherein the method further comprises: recording a representation of the content in an encrypted form in response to a message from the first conditional access server (column 2, lines 10-21, column 6, lines 35-52, column 7, lines 30-51, column 8, lines 16-31 and 51-62, column 9, lines 3-20, column 10, lines 19-29 and 37-46 and column 11, lines 26-47).

23. Regarding claim 12, Grimes discloses wherein the client sends a request, through a network connection to the second conditional access server, for authorization to present the content after the first conditional access server provides at least a portion of the content which is recorded; the second conditional access server obtains authorization from the first conditional access server, after the first conditional access server provides the portion of the content, for said authorizing (column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

24. Regarding claim 13, Grimes discloses wherein the method further comprises: translating authorization to access the content from authorization received from the first conditional access server to authorization for the client (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

25. Regarding claim 16, Grimes discloses wherein the first conditional access server provides authorization to the second conditional access server according to an identity of the second conditional access server; the second conditional access server provides authorization to the client according to an identity of the client (column 3, lines 29-41, column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18);

the first conditional access server is not aware of an identity of the client (column 7, lines 40-51, “generating a digital certificate 84 may be performed by the third-party website server (e.g., when the user orders content from a third-party website)").

26. Regarding claim 18, Grimes discloses wherein the second conditional access server is a server of a further secondary conditional access server and acts as a primary conditional access server with respect to the further secondary conditional access server (column 7, lines 18-23, “the DRM server 58 or other server at the NOC 12”, column 8, lines 16-31, “third-party website server” and column 9, lines 3-11).

27. Regarding claims 19 and 23, Grimes discloses a secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

a communication interface, the communication interface to receive a first set of cryptographic keys from a primary conditional access server which provides a

IPR2025-00305
ASUS EX1002 Page 398

representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys (column 2, lines 10-39, "computer-readable medium further comprises instructions for requesting the encryption key from a digital rights management (DRM) server using a digital certificate", column 4, lines 29-49, column 5, lines 53-65, column 7, lines 11-29 and column 13, lines 4-18);

a controller coupled to the communication interface, the controller to authorize a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server; wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content (column 7, lines 11-29, "if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content", column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

28. Grimes significantly discloses the claimed invention, as cited above. However, Grimes does not substantially disclose the claim language pertaining to "wherein the primary conditional access server authenticates clients of the primary conditional access server through a first authentication process and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process". Simelius discloses said claim language, as cited below.

29. Regarding claims 19 and 23, Simelius discloses wherein the primary conditional access server authenticates clients of the primary conditional access server through a first authentication process and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, "second parent client" and lines 60-65, "first parent client", column 14, lines 18-37 and column 15, lines 42-53).

30. The motivation to combine would be "This provides a solution for more flexible use of digital content across a plurality of devices, while the use cannot be freely copied." (*Simelius* – column 7, lines 63-65).

31. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Simelius with the teachings of Grimes so that "the exchange of rights to access digital content between devices will facilitate a user-friendly environment in any situation for consuming the digital content" (*Simelius* – column 7, lines 65-67).

32. Regarding claim 21, Grimes discloses wherein the second set of cryptographic keys comprises a key of a digital rights management system; the client comprises a digital rights management client; the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines

14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

33. Regarding claims 22 and 26, Grimes discloses wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of the client (column 3, lines 29-41, column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18);

the primary conditional access server is not aware of an identity of the client (column 7, lines 40-51, “generating a digital certificate 84 may be performed by the third-party website server (e.g., when the user orders content from a third-party website)").

34. Regarding claim 24, Grimes discloses means for recording a representation of the content in an encrypted form in response to a message from the primary conditional access server. wherein the client sends a request, through a network connection to the secondary conditional access server, for authorization to present the content after the primary conditional access server provides at least a portion of the content which is recorded; the secondary conditional access server obtains authorization from the primary conditional access server, after the primary conditional access server provides

IPR2025-00305
ASUS EX1002 Page 401

the portion of the content, for authorizing the client to present the content (column 7, lines 7-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

35. Regarding claim 25, Grimes discloses means for translating authorization to access the content from authorization received from the primary conditional access server to authorization for the client. wherein the second set of cryptographic keys comprises a key of a digital rights management system; the client comprises a digital rights management client; wherein the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

36. Regarding claims 28 and 62, Grimes teaches a method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component; broadcasting the media component from a first conditional access server; receiving a client request to use the media component from a client through a second conditional access server after said broadcasting; responding to

the client request through the second conditional access server (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

37. Regarding claims 28 and 62, Simelius teaches wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process and the second conditional access server authenticates clients of the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

38. Regarding claims 29, 63 and 97, Grimes teaches broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request (column 7, lines 7-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

39. Regarding claims 30, 64 and 98, Grimes teaches wherein the client is not authorized to use the portion of the media content before the second entitlement management message (column 11, lines 3-19, "validation refused" and column 13, lines

4-18, "the hardware profile will not match the user machine 40 of client 18 if the user has made an unauthorized transfer of the client software 43").

40. Regarding claims 31, 65 and 99, Grimes teaches wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously (column 3, lines 61-67, column 4, lines 1-9, “this stored or personal content 28 may be kept on a user machine hard-drive or other storage medium” and 42-59 and column 5, lines 1-18).

41. Regarding claims 32, 66, 100 and 130, Grimes teaches a method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

processing the security messages on the conditional access server (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

42. Grimes significantly teaches the claim language, as cited above, but it does not substantially teach the claim language pertaining to “wherein the primary security

system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process". Simelius teaches said claim language, as cited below.

43. Regarding claims 32, 66, 100 and 130, Simelius teaches wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, "second parent client" and lines 60-65, "first parent client", column 14, lines 18-37 and column 15, lines 42-53).

44. The motivation to combine would be "This provides a solution for more flexible use of digital content across a plurality of devices, while the use cannot be freely copied." (*Simelius* – column 7, lines 63-65).

45. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Simelius with the teachings of Grimes so that "the exchange of rights to access digital content between devices will facilitate a user-friendly environment in any situation for consuming the digital content" (*Simelius* – column 7, lines 65-67).

46. The claim language within claims 48, 82, 96, 116 and 140 are analogous to the claim language above; thus the motivation and obviousness to combine for claims 32, 66, 100 and 130 will also pertain to claims 48, 82, 96, 116 and 140.

47. Regarding claims 33, 67 and 101, Grimes teaches wherein the security messages comprise entitlement management messages;

the conditional access server has a user key representing a subscriber of the primary security system (column 6, lines 65-67, column 7, lines 1-29 and column 8, lines 43-50);

said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system (column 9, lines 24-60).

48. Regarding claims 34, 68 and 102, Grimes teaches wherein the access controlled data is protected using a digital rights management system (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

49. Regarding claims 35, 69, 103 and 132, Grimes teaches wherein rights to the access controlled data are at least partially derived from the entitlement management messages (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

50. Regarding claims 38, 72, 106 and 134, Grimes teaches receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system (column 12, lines 26-61 and column 13, lines 19-25 and 28-30);

descrambling the scrambled content according to the entitlement control message; wherein the access controlled data comprises a result of descrambling the scrambled content (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

51. Regarding claims 39, 73, 107 and 135, Grimes teaches storing, at the conditional access server, the content in an encrypted form; wherein the access controlled data is provided in response to a request from the secondary conditional access client (column 2, lines 10-21, column 6, lines 35-52, column 7, lines 30-51, column 8, lines 16-31 and 51-62, column 9, lines 3-20, column 10, lines 19-29 and 37-46 and column 11, lines 26-47).

52. Regarding claims 40, 74, 108, 136, Grimes teaches receiving, at the conditional access server, an entitlement control message of the primary security system; processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message; wherein the access controlled data comprises the substitutive entitlement control message (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

53. Regarding claims 48, 82 and 116, Grimes teaches a method to process media content provided by a primary security system, the method comprising:
receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary

security system (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

54. Regarding claims 48, 82 and 116, Simelius teaches wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

55. Regarding claims 49, 83, 117 and 141, Grimes teaches wherein the security message is an entitlement message; wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system (column 7, lines 40-51, “generating a digital certificate 84 may be performed by the third-party website server (e.g., when the user orders content from a third-party website)", column 11, lines 3-19, "validation refused" and column 13, lines 4-18, "the hardware profile will not match the user machine 40 of client 18 if the user has made an unauthorized transfer of the client software 43").

56. Regarding claims 50, 84, 118 and 142, Grimes teaches wherein the access controlled format protects access to data using a digital rights management system (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines

38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

57. Regarding claims 51, 85 and 119, Grimes teaches automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data (column 12, lines 26-61 and column 13, lines 19-25 and 28-30);

descrambling and recording the portion of the media content in response to a determination to descramble (column 12, lines 62-67 and column 13, lines 1-3 and 25-28);

recording the portion of the media content without descrambling in response to a determination not to descramble (column 12, lines 26-61 and column 13, lines 19-25 and 28-30).

58. Regarding claims 57, 91 and 125, Grimes teaches wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

59. Regarding claims 58, 92 and 126, Grimes teaches receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

60. Regarding claims 59, 93 and 127, Grimes teaches wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; the method further comprises: storing the second entitlement control message with the portion of the media content (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

61. Regarding claim 96, Grimes discloses a primary security system to provide conditional access, the method comprising:

means for broadcasting a first entitlement management message for a subscriber to request caching of a media component; broadcasting the media component from a first conditional access server; receiving a client request to use the media component from a client through a second conditional access server after said broadcasting; responding to the client request through the second conditional access server (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

62. Regarding claim 96, Simelius discloses wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

63. Regarding claim 131, Grimes discloses wherein the security messages comprise entitlement management messages; the access controlled data is protected using a digital rights management system (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

64. Regarding claim 140, Grimes discloses a secondary conditional access client, comprising:

a communication interface to receive, from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system;

a processor coupled to the communication interface, the processor to process the access controlled data (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

65. Regarding claim 140, Simelius discloses wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

66. Regarding claim 143, Grimes discloses wherein the processor is to automatically determine whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data (column 12, lines 26-61 and column 13, lines 19-25 and 28-30);

the client further comprises:

a storage device; a descrambler coupled to the processor and the storage device, in response to a determination to descramble the descrambler to descramble the portion of the media content for storing in the storage device, in response to a determination not to descramble the storage device to record the portion of the media content without descrambling (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

67. Regarding claim 146, Grimes discloses a physical interface to receive a first entitlement control message for descrambling a portion of media content received from the primary security system (column 12, lines 62-67 and column 13, lines 1-3 and 25-28);

and wherein the communication interface is to send the first entitlement control message to the conditional access server through a network connection (column 3, lines 29-41, column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

68. Claims 36, 41-47, 52-56, 60, 61, 70, 75-81, 86-90, 94, 95, 104, 109-115, 120-124, 128, 129, 133, 137-139, 144 and 145 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grimes and Simelius, as applied to claims 32, 66, 100, 130 and 140 above, and further in view of United States Patent No. 7,302,058 to Candelore, hereinafter Candelore.

69. Grimes and SImelius significantly teach the claimed invention, as cited above. However, Grimes and Simelius do not substantially teach the claim language in the following claims pertaining to "control words". Candelore teaches said claim language, as cited below.

70. The motivation to combine would be that "the control word is only decrypted in descrambler IC 440 that actually uses the control word, therefore, the control word is never exposed, and cannot be obtained by hackers". (*Candelore* – column 6, lines 42-49).

71. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Candelore with the teachings of Grimes and Simelius so that "Local Access control can be performed by the Insecure Processor because the critical 'secure' function is isolated in the Descrambler IC" (*Candelore* – column 10, lines 48-54).

72. Regarding claims 36, 70, 104 and 133, Candelore teaches receiving, at the conditional access server, an entitlement control message of the primary security system (column 3, lines 61-67, column 4, lines 1-14 and 55-67 and column 5, lines 1-3 and 20-26);

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system (column 5, lines 20-26 and column 6, lines 11-31 and 42-51);

wherein the access controlled data comprises the control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

73. Regarding claims 37, 71 and 105, Candelore teaches wherein the access controlled data comprises a decrypted version of the entitlement control message (column 4, lines 6-14, column 6, lines 32-49 and column 7, lines 25-41).

74. Regarding claims 41, 75, 109 and 137, Candelore teaches wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server (column 3, lines 15-23, column 6, lines 11-31, “encrypts the CWs in encryption block 414 with keys that are unique to transport descrambler integrated circuit (IC) 440” and column 7, lines 54-62).

75. Regarding claims 42, 76 and 110, Candelore teaches wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system (column 4, lines 9-13 and column 6, lines 11-20 and 42-49).

76. Regarding claims 43, 77 and 111, Candelore teaches wherein the entitlement control message and the substitutive entitlement control message have a same control word (Figure 2, element 416 and Figure 3, elements 41, 44 and 45, column 3, lines 15-

23, column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

77. Regarding claims 44, 78 and 112, Candelore teaches wherein the entitlement control message has a first control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41);

the substitutive entitlement control message has a second control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

the first and second control words are different (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61).

78. Regarding claims 45, 79 and 113, Candelore teaches wherein the access controlled data further comprises the first and second control words (Figure 6, "encrypted control word A" and "encrypted control word B" and column 7, lines 42-61).

79. Regarding claims 46, 80, 114 and 138, Candelore teaches receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word (column 3, lines 15-24 and column 6, lines 14-17 and 60-63);

generating a second entitlement control message containing a second control word that is different from the first control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

descrambling the content using the first control word and rescrambling the content by the second control word (column 6, lines 11-20, column 7, lines 54-67 and column 8, lines 1-23);

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message (column 5, lines 55-65).

80. Regarding claims 47, 81 and 115, Candelore teaches storing, at the conditional access server, the content rescrambled by the second control word (column 5, lines 55-65);

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client (column 5, lines 55-65 and column 6, lines 1-10).

81. Regarding claims 52, 86, 120 and 144, Candelore teaches sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form (column 5, lines 20-26 and column 6, lines 11-31 and 42-51);

wherein the access controlled data comprises the control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, and column 7, lines 25-41).

82. Regarding claims 53, 87 and 121, Candelore teaches descrambling media content using the control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, “conditional access unit 401

will decrypt the control words and use the clear control words to descramble the program content" and column 7, lines 25-41);

storing the media content in a storage under protection of a digital rights management system (column 6, lines 11-31 and 42-51).

83. Regarding claims 54, 88 and 122, Candelore teaches descrambling media content using the control word; and rendering the media content for presentation (column 6, lines 11-63, "conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content" and column 7, lines 25-41).

84. Regarding claims 55, 89 and 123, Candelore teaches retrieving the entitlement control message from a storage device (column 6, lines 11-31 and 42-51);

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client (column 3, lines 61-67, column 4, lines 1-14 and 55-67 and column 5, lines 1-3 and 20-26).

85. Regarding claims 56, 90 and 124, Candelore teaches wherein the access controlled data comprises a decrypted version of the entitlement control message (column 6, lines 11-63, "conditional access unit 401 will decrypt the control words and

use the clear control words to descramble the program content" and column 7, lines 25-41).

86. Regarding claims 60, 94 and 128, Candelore teaches wherein both the first and the second entitlement control messages contain a same control word (Figure 2, element 416 and Figure 3, elements 41, 44 and 45, column 3, lines 15-23, column 6, lines 11-63, "conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content" and column 7, lines 25-41);
the second entitlement control message is encrypted to be decrypted using a key of the conditional access server (column 4, lines 6-14, column 6, lines 32-49 and column 7, lines 25-41).

87. Regarding claims 61, 95 and 129, Candelore teaches wherein the first entitlement control message contains a first control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 3, lines 15-24 and column 6, lines 14-17 and 60-63);
the second entitlement control message contains a second control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);
the first and second control words are different (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);
the access controlled data further comprises the first and second control words (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);
the method further comprises: descrambling the content using the first control word and rescrambling the content using the second control word (column 5, lines 55-65).

88. Regarding claim 139, Candelore discloses a storage device coupled to the transcrambler, the storage device to store the content rescrambled by the second control word (column 5, lines 55-65).

89. Regarding claim 145, Candelore discloses a storage device;

a descrambler coupled to the processor and the storage device, the descrambler to descramble media content using the control word, the storage device to store the media content under protection of a digital rights management system (column 6, lines 11-63, "conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content" and column 7, lines 25-41).

Conclusion

90. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

91. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

92. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

93. The following United States Patents and Patent Application Publication are cited to further show the state of the art with respect to the access control of content, such as:

United States Patent No. 7,127,619 to Unger et al., which is cited to show the decoding and decryption of partially encrypted information.

United States Patent No. 7,171,558 to Mourad et al., which is cited to show transparent digital rights management for extendible content viewers.

United States Patent No. 7,177,429 to Moskowitz et al., which is cited to show system and methods for permitting open access to data objects and for securing data within the data objects.

United States Patent No. 7,292,692 to Bonan et al., which is cited to show content scrambling with minimal impact on legacy devices.

United States Patent No. 7,316,032 to Tayebi et al., which is cited to show a method for allowing a customer to preview, acquire and/or pay for the information and a system therefor.

United States Patent No. 7,336,784 to Zuili which is cited to show a multimedia decoder method and system with authentication and enhanced digital rights management (DRM) where each received signal is unique and where the missing signal is cached inside the storage memory of each receiver.

United States Patent Application Publication No. US 2004/0196842 to Dobbins which is cited to show a method and system for according preferred transport based on node identification.

United States Patent No. 7,296,154 to Evans et al., which is cited to show secure media path methods, systems and architectures.j

United States Patent No. 7,174021 to Krishnaswamy et al., which is cited to show systems and methods for providing secure server key operations.

94. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

95. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

96. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/007,116	Applicant(s)/Patent Under Reexamination VANTALON ET AL.	
	Examiner JEREMIAH AVERY	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,036,011	04-2006	Grimes et al.	713/156
*	B	US-7,302,058	11-2007	Candelore, Brant L.	380/200
*	C	US-7,127,619	10-2006	Unger et al.	713/193
*	D	US-7,171,588	01-2007	Friedman et al.	714/38
*	E	US-7,177,429	02-2007	Moskowitz et al.	380/252
*	F	US-7,292,692	11-2007	Bonan et al.	380/212
*	G	US-7,316,032	01-2008	Tayebi et al.	705/51
*	H	US-7,336,784	02-2008	Zuili, Patrick	380/200
*	I	US-7,493,291	02-2009	Simelius, Kim	705/59
*	J	US-2004/0196842	10-2004	Dobbins, Kurt A.	370/389
*	K	US-7,296,154	11-2007	Evans et al.	713/169
*	L	US-7,174,021	02-2007	Krishnaswamy et al.	380/277
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1058	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
L2	932	L1 and server	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
L3	556	L2 and unauthori$	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
L4	477	L3 and (authoris$ or authoriz$)	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
L5	461	L4 and (ID or identit$ or identif$)	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
L6	448	L5 and ((first or primary) or (second$ or other) near server)	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
L7	448	L6 and ((first or primary) or (second$ or other) near (authentic$ or verify$ or verification))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:02
L8	448	L7 and ((first or primary) or (second$ or other or next) near ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:06

L9	0	L8 and (((first or primary) or (second$ or other or next) near (access near server)) near ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:08
L10	7	L8 and (((first or primary) or (second$ or other or next) near (access near server)) same ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:09
L11	7	L8 and (((first or primary) or (second$ or other or next) near server) same ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:22
L12	0	L8 and (((first or primary) or (second$ or other or next) near server) near ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:23
L13	55	L8 and (((first or primary) or (second$ or other or next) near server) near (authentic$ or verify$ or verification))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:24
L14	11	L13 and ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:25

S1	990	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT	OR	ON	2009/03/26 19:43
S2	873	S1 and server	US-PGPUB; USPAT	OR	ON	2009/03/26 19:48
S3	522	S2 and unauthori$	US-PGPUB; USPAT	OR	ON	2009/03/26 19:49
S4	447	S3 and (authoris$ or authoriz$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:49
S5	433	S4 and (ID or identit$ or identif$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:50
S6	420	S5 and ((first or primary) or (second$ or other) near server)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:50
S7	402	S6 and (broadcast$ or transmit$ or transmission or send$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:52
S8	395	S7 and ((broadcast$ or transmit$ or transmission or send$) same (media or audio or video or stream or content or data or information))	US-PGPUB; USPAT	OR	ON	2009/03/26 19:52
S9	317	S8 and (play$ or playback)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:53
S10	150	S9 and (subscribe$ or subscript$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:54
S11	39	S10 and $2scrambl$	US-PGPUB; USPAT	OR	ON	2009/03/26 19:54
S12	7	S11 and (control$5 near word)	US-PGPUB; USPAT	OR	ON	2009/03/26 20:00

11/21/2009 1:24:39 PM
C:\Documents and Settings\javery\My Documents\EAST\Workspaces\11007116.wsp

IPR2025-00305
ASUS EX1002 Page 426

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	11/21/2009								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	11/21/2009								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	46	✓								
	47	✓								
	48	✓								
	49	✓								
	50	✓								
	51	✓								
	52	✓								
	53	✓								
	54	✓								
	55	✓								
	56	✓								
	57	✓								
	58	✓								
	59	✓								
	60	✓								
	61	✓								
	62	✓								
	63	✓								
	64	✓								
	65	✓								
	66	✓								
	67	✓								
	68	✓								
	69	✓								
	70	✓								
	71	✓								
	72	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	11/21/2009								
	73	✓								
	74	✓								
	75	✓								
	76	✓								
	77	✓								
	78	✓								
	79	✓								
	80	✓								
	81	✓								
	82	✓								
	83	✓								
	84	✓								
	85	✓								
	86	✓								
	87	✓								
	88	✓								
	89	✓								
	90	✓								
	91	✓								
	92	✓								
	93	✓								
	94	✓								
	95	✓								
	96	✓								
	97	✓								
	98	✓								
	99	✓								
	100	✓								
	101	✓								
	102	✓								
	103	✓								
	104	✓								
	105	✓								
	106	✓								
	107	✓								
	108	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	11/21/2009								
	109	✓								
	110	✓								
	111	✓								
	112	✓								
	113	✓								
	114	✓								
	115	✓								
	116	✓								
	117	✓								
	118	✓								
	119	✓								
	120	✓								
	121	✓								
	122	✓								
	123	✓								
	124	✓								
	125	✓								
	126	✓								
	127	✓								
	128	✓								
	129	✓								
	130	✓								
	131	✓								
	132	✓								
	133	✓								
	134	✓								
	135	✓								
	136	✓								
	137	✓								
	138	✓								
	139	✓								
	140	✓								
	141	✓								
	142	✓								
	143	✓								
	144	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	11/21/2009								
	145	✓								
	146	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

SEARCHED			
Class	Subclass	Date	Examiner
none	none	11/21/2009	JLA

SEARCH NOTES		
Search Notes	Date	Examiner
Updated EAST Search	11/21/2009	JLA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
none	none	11/21/2009	JLA

REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL

Address to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450

Application No. 11/007,116
Filing Date 12/07/2004
First Named Inventor Luc Vantalon, et al.
Art Unit 2431
Examiner Name Avery, Jeremiah L.
Attorney Docket No. 06517.P002

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See instruction sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. **Submission required under 37 C.F.R. § 1.114** – Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. [ ] Previously submitted If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. [ ] Consider the amendment(s)/reply under 37 C.F.R. § 1.116 previously filed on _____ (Any unentered amendment(s) referred to above will be entered. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      ii. [ ] Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      iii. [ ] Other _____

   b. [X] Enclosed

      i. [X] Amendment/Reply
      ii. [ ] Affidavit(s)/Declaration(s)
      iii. [ ] Information Disclosure Statement (IDS)
      iv. [ ] Other: _____

2. **Miscellaneous**

   a. [ ] Suspension of action on the above-identified application is requested under 37 C.F.R. § 1.103(c) for a period of _____ months.(Period of suspension shall not exceed 3 months. **Fee under 37 C.F.R. § 1.17(i) required)**

   b. [ ] Other: _____

3. **Fees** The RCE fee under 37 C.F.R. § 1.17(e) is required by C.F.R. § 1.114 when the RCE is filed.

   a. [X] The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. 02-2666

      i. [X] RCE fee required under 37 C.F.R. § 1.17(e)
      ii. [ ] Extension of time fee (37 C.F.R. §§ 1.136 and 1.17)
      iii. [ ] Processing fee under 37 CFR § 1.17(i) for Limited Suspension of Action
      iv. [ ] Other _____

   b. [ ] Check in the amount of $_____ is enclosed

   c. [ ] Payment by credit card (Form PTO-2038 enclosed)

      WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name (Print/Type) James C. Scheller, Jr. Registration No. (Attorney/Agent) 31,195

Signature _____ Date March 2, 2010

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

March 2, 2010
Date of Deposit

Connie Thayer
Name of Person Filing Correspondence

Connie Thayer 3-2-10
Signature Date

Based on Form PTO/SB/30 (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03

IPR2025-00305
ASUS EX1002 Page 433

Atty. Docket No. 06517.P002 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Luc Vantalon, et al.	)	Examiner: Avery, Jeremiah L.
	)	
Application No. 11/007,116	)	Art Unit: 2431
	)	
Filed: December 7, 2004	)	
	)	Confirmation No. 9254
For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

Dear Sir:

In response to the Office Action dated December 8, 2009, Applicant respectfully requests that the above-identified application be amended as follows and that the accompanying RCE be entered and that the following remarks be considered.

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

March 2, 2010
Date of Deposit

Connie Thayer
Name of Person Filing Correspondence

Connie Thayer
Signature

3-2-10
Date

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) A method to control a presentation of content, the method comprising:

receiving a representation of content from a first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access; and

presenting the content, at a user's request, through a second conditional access server which is coupled to the first conditional access server;

wherein the presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively;

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content; and

wherein the first conditional access server authenticates ~~clients~~ client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates ~~clients~~ client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

2. (Original) The method of claim 1, wherein the content is presented by a network client of the second conditional access server using the second set of cryptographic keys.

3. (Original) The method of claim 2, wherein the first conditional access server provides the second conditional access server the first set of cryptographic keys for authorized use.

4. (Original) The method of claim 3, wherein the user's request is after the first conditional access server provides at least a portion of the content; and the portion of the content is presented in response to the user's request.

5. (Original) The method of claim 2, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the network client is a digital rights management client.

6. (Original) The method of claim 5, wherein the second conditional access server authorizes the network client to use the content through the digital rights management system in accordance with authorization to use received from the first conditional access server.

7. (Original) The method of claim 1, wherein the second conditional access server translates authorization to access the content from authorization received from the first conditional access server to authorization for the network client.

8. (Original) The method of claim 1, wherein the second set of cryptographic keys consists one key.

9. (Original) The method of claim 1, wherein the second conditional access server acts as a primary conditional access server to another secondary conditional access server.

10. (Currently Amended) A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content, the method comprising:

receiving, at a second conditional access server, a first set of cryptographic keys from a first conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys; and

authorizing a client of the second conditional access server to present the content in accordance with authorization the second conditional access server received from the first conditional access server;

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content; and

wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

11. (Original) The medium of claim 10, wherein the method further comprises:

recording a representation of the content in an encrypted form in response to a message from the first conditional access server.

12. (Original) The medium of claim 11, wherein the client sends a request, through a network connection to the second conditional access server, for authorization to present the content after the first conditional access server provides at least a portion of the content which is recorded; and the second conditional access server obtains authorization from the first conditional access server, after the first conditional access server provides the portion of the content, for said authorizing.

13. (Original) The medium of claim 10, wherein the method further comprises:

translating authorization to access the content from authorization received from the first conditional access server to authorization for the client.

14. (Original) The medium of claim 13, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the client comprises a digital rights management client.

15. (Original) The medium of claim 14, wherein the second conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the first conditional access server.

16. (Original) The medium of claim 15, wherein the first conditional access server provides authorization to the second conditional access server according to an identity of the second conditional access server; the second conditional access server provides

authorization to the client according to an identity of the client; and the first conditional access server is not aware of an identity of the client.

17. (Original) The medium of claim 10, wherein the second set of cryptographic keys consists one key.

18. (Original) The medium of claim 10, wherein the second conditional access server is a server of a further secondary conditional access server and acts as a primary conditional access server with respect to the further secondary conditional access server.

19. (Currently Amended) A secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

a communication interface, the communication interface to receive a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys; and

a controller coupled to the communication interface, the controller to authorize a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server;

wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content, and

wherein the primary conditional access server authenticates clients of the primary conditional access server through a first authentication process using a first root of trust and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

20. (Original) The secondary conditional access server of claim 19, wherein the controller is to translate authorization to access the content from authorization received from the primary conditional access server to authorization for the client.

21. (Original) The secondary conditional access server of claim 20, wherein the second set of cryptographic keys comprises a key of a digital rights management system; the client comprises a digital rights management client; and the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server.

22. (Original) The secondary conditional access server of claim 20, wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of

the client; and the primary conditional access server is not aware of an identity of the client.

23. (Currently Amended) A secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

means for receiving a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys; and

means for authorizing a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server;

wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content, and

wherein the primary conditional access server authenticates clients of the primary conditional access server through a first authentication process using a first root of trust and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

24. (Previously Presented) The secondary conditional access server of claim 23, further comprising:

means for recording a representation of the content in an encrypted form in response to a message from the primary conditional access server,

wherein the client sends a request, through a network connection to the secondary conditional access server, for authorization to present the content after the primary conditional access server provides at least a portion of the content which is recorded; and

the secondary conditional access server obtains authorization from the primary conditional access server, after the primary conditional access server provides the portion of the content, for authorizing the client to present the content.

25. (Previously Presented) The secondary conditional access server of claim 23, further comprising:

means for translating authorization to access the content from authorization received from the primary conditional access server to authorization for the client,

wherein the second set of cryptographic keys comprises a key of a digital rights management system; and

the client comprises a digital rights management client; and

wherein the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server.

26. (Original) The secondary conditional access server of claim 23, wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of the client; and the primary conditional access server is not aware of an identity of the client.

27. (Original) The secondary conditional access server of claim 23, wherein the second set of cryptographic keys consists one key.

28. (Currently Amended) A method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component;

broadcasting the media component from a first conditional access server;

receiving a client request to use the media component from a client ~~through~~ of a second conditional access server after said broadcasting; and

responding to the client request ~~through~~ from the client of the second conditional access server,

wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second

authentication process uses a second root of trust which is independent of and different than the first root of trust.

29. (Original) The method of claim 28, further comprising:

broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

30. (Original) The method of claim 29, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

31. (Original) The method of claim 30, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

32. (Currently Amended) A method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system;

processing the security messages on the conditional access server; and

transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

33. (Original) The method of claim 32, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system.

34. (Original) The method of claim 32, wherein the access controlled data is protected using a digital rights management system.

35. (Original) The method of claim 34, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

36. (Original) The method of claim 34, further comprising:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

37. (Original) The method of claim 36, wherein the access controlled data comprises a decrypted version of the entitlement control message.

38. (Original) The method of claim 34, further comprising:

receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

39. (Original) The method of claim 38, further comprising:

storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

40. (Original) The method of claim 32, further comprising:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

41. (Original) The method of claim 40, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

42. (Original) The method of claim 41, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

43. (Original) The method of claim 41, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

44. (Original) The method of claim 41, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

45. (Original) The method of claim 44, wherein the access controlled data further comprises the first and second control words.

46. (Original) The method of claim 32, further comprising:

receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

generating a second entitlement control message containing a second control word that is different from the first control word; and

descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

47. (Original) The method of claim 46, further comprising:

storing, at the conditional access server, the content rescrambled by the second control word; and

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

48. (Currently amended) A method to process media content provided by a primary security system, the method comprising:

receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system,

wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

49. (Original) The method of claim 48, wherein the security message is an entitlement message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

50. (Original) The method of claim 48, wherein the access controlled format protects access to data using a digital rights management system.

51. (Original) The method of claim 50, further comprising:

automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

descrambling and recording the portion of the media content in response to a determination to descramble; and

recording the portion of the media content without descrambling in response to a determination not to descramble.

52. (Original) The method of claim 50, further comprising:

sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

53. (Original) The method of claim 52, further comprising:

descrambling media content using the control word; and

storing the media content in a storage under protection of a digital rights management system.

54. (Original) The method of claim 52, further comprising:

descrambling media content using the control word; and

rendering the media content for presentation.

55. (Original) The method of claim 54, further comprising:

retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary

conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

56. (Original) The method of claim 52, wherein the access controlled data comprises a decrypted version of the entitlement control message.

57. (Original) The method of claim 50, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

58. (Original) The method of claim 48, further comprising:

receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

59. (Original) The method of claim 58, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the method further comprises:

storing the second entitlement control message with the portion of the media content.

60. (Original) The method of claim 59, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

61. (Original) The method of claim 59, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further comprises:

descrambling the content using the first control word and rescrambling the content using the second control word.

62. (Currently Amended) A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component;

broadcasting the media component from a first conditional access server;

receiving a client request to use the media component from a client ~~through~~ of a second conditional access server after said broadcasting; and

responding to the client request ~~through~~ from the client of the second conditional access server,

wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process using a first root of trust and

the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

63. (Original) The medium of claim 62, wherein the method further comprises:

broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

64. (Original) The medium of claim 63, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

65. (Original) The medium of claim 64, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

66. (Currently amended) A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system;

processing the security messages on the conditional access server; and

transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

67. (Original) The medium of claim 66, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system.

68. (Original) The medium of claim 66, wherein the access controlled data is protected using a digital rights management system.

69. (Original) The medium of claim 68, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

70. (Original) The medium of claim 68, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

71. (Original) The medium of claim 70, wherein the access controlled data comprises a decrypted version of the entitlement control message.

72. (Original) The medium of claim 68, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

73. (Original) The medium of claim 72, wherein the method further comprises:

storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

74. (Original) The medium of claim 66, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

75. (Original) The medium of claim 74, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

76. (Original) The medium of claim 75, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

77. (Original) The medium of claim 75, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

78. (Original) The medium of claim 75, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

79. (Original) The medium of claim 78, wherein the access controlled data further comprises the first and second control words.

80. (Original) The medium of claim 66, wherein the method further comprises:

receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

generating a second entitlement control message containing a second control word that is different from the first control word; and

descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

81. (Original) The medium of claim 80, wherein the method further comprises:

storing, at the conditional access server, the content rescrambled by the second control word; and

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

82. (Currently amended) A machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process media content provided by a primary security system, the method comprising:

receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system,

wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

83. (Original) The medium of claim 82, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

84. (Original) The medium of claim 82, wherein the access controlled format protects access to data using a digital rights management system.

85. (Original) The medium of claim 84, wherein the method further comprises:

automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

descrambling and recording the portion of the media content in response to a determination to descramble; and

recording the portion of the media content without descrambling in response to a determination not to descramble.

86. (Original) The medium of claim 84, wherein the method further comprises:

sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

87. (Original) The medium of claim 86, wherein the method further comprises:

descrambling media content using the control word; and

storing the media content in a storage under protection of a digital rights management system.

88. (Original) The medium of claim 86, wherein the method further comprises:

descrambling media content using the control word; and

rendering the media content for presentation.

89. (Original) The medium of claim 88, wherein the method further comprises:

retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

90. (Original) The medium of claim 86, wherein the access controlled data comprises a decrypted version of the entitlement control message.

91. (Original) The medium of claim 84, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

92. (Original) The medium of claim 82, wherein the method further comprises:

receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

93. (Original) The medium of claim 92, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the method further comprises:

storing the second entitlement control message with the portion of the media content.

94. (Original) The medium of claim 93, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

95. (Original) The medium of claim 93, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further comprises:

descrambling the content using the first control word and rescrambling the content using the second control word.

96. (Currently Amended) A primary security system to provide conditional access, the system comprising:

means for broadcasting a first entitlement management message for a subscriber to request caching of a media component;

means for broadcasting the media component;

means for receiving a client request to use the media component from a client ~~through~~ of a secondary conditional access server after said broadcasting; and

means for responding to the client request ~~through~~ from the client of the secondary conditional access server,

wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

97. (Original) The system of claim 96, further comprising:

means for broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

98. (Original) The system of claim 97, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

99. (Original) The system of claim 98, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

100. (Currently amended) A data processing system to process conditional access protection, the data processing system comprising:

means for receiving, at a conditional access server, security messages of a primary security system;

means for processing the security messages on the conditional access server; and

means for transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

101. (Previously Presented) The data processing system of claim 100, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said means for processing the entitlement management messages comprises:

means for decrypting to obtain a service key of the primary security system.

102. (Original)The data processing system of claim 100, wherein the access controlled data is protected using a digital rights management system.

103. (Original)The data processing system of claim 102, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

104. (Original)The data processing system of claim 102, further comprising:

means for receiving, at the conditional access server, an entitlement control message of the primary security system; and

means for processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

105. (Original)The data processing system of claim 104, wherein the access controlled data comprises a decrypted version of the entitlement control message.

106. (Original)The data processing system of claim 102, further comprising:

means for receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

means for descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

107. (Original)The data processing system of claim 106, further comprising:

means for storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

108. (Original)The data processing system of claim 100, further comprising:

means for receiving, at the conditional access server, an entitlement control message of the primary security system; and

means for processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

109. (Original)The data processing system of claim 108, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

110. (Original)The data processing system of claim 109, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

111. (Original)The data processing system of claim 109, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

112. (Original)The data processing system of claim 109, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

113. (Original)The data processing system of claim 112, wherein the access controlled data further comprises the first and second control words.

114. (Original)The data processing system of claim 100, further comprising:

means for receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

means for generating a second entitlement control message containing a second control word that is different from the first control word; and

means for descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

115. (Original)The data processing system of claim 114, further comprising:

means for storing, at the conditional access server, the content rescrambled by the second control word; and

means for retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

116. (Currently amended) A data processing system to process media content provided by a primary security system, the data processing system comprising:

means for receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system,

wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

117. (Original)The data processing system of claim 116, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

118. (Original)The data processing system of claim 116, wherein the access controlled format protects access to data using a digital rights management system.

119. (Original)The data processing system of claim 118, further comprising:

means for automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

means for descrambling and recording the portion of the media content in response to a determination to descramble; and

means for recording the portion of the media content without descrambling in response to a determination not to descramble.

120. (Original)The data processing system of claim 118, further comprising:

means for sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

121. (Original)The data processing system of claim 120, further comprising:

means for descrambling media content using the control word; and

means for storing the media content in a storage under protection of a digital rights management system.

122. (Original)The data processing system of claim 120, further comprising:

means for descrambling media content using the control word; and

means for rendering the media content for presentation.

123. (Original)The data processing system of claim 122, further comprising:

means for retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

124. (Original)The data processing system of claim 120, wherein the access controlled data comprises a decrypted version of the entitlement control message.

125. (Original)The data processing system of claim 118, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

126. (Original)The data processing system of claim 116, further comprising:

means for receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

means for sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

127. (Original)The data processing system of claim 126, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the system further comprises:

means for storing the second entitlement control message with the portion of the media content.

128. (Original)The data processing system of claim 127, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

129. (Original)The data processing system of claim 127, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the system further comprises:

means for descrambling the content using the first control word and rescrambling the content using the second control word.

130. (Currently amended) A conditional access server, comprising:

one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system;

a processor coupled to the one or more communication interfaces, the processor to process the security messages, and the one or more communication interfaces to transmit, to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

131. (Original)The conditional access server of claim 130, wherein the security messages comprise entitlement management messages; and the access controlled data is protected using a digital rights management system.

132. (Original)The conditional access server of claim 131, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

133. (Original)The conditional access server of claim 131, wherein the one or more communication interfaces are to receive an entitlement control message of the primary security system; the processor is to obtain a control word of the primary security system from the entitlement control message; and the access controlled data comprises the control word.

134. (Original)The conditional access server of claim 131, wherein the one or more communication interfaces are to receive an entitlement control message and scrambled content of the primary security system; and the conditional access server further comprises:

a descrambler coupled to the processor, the descrambler to descramble the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

135. (Original)The conditional access server of claim 134, further comprising:

a storage device coupled to one or more communication interfaces, the storage device to store the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

136. (Previously Presented) The conditional access server of claim 130, wherein the one or more communication interfaces are to receive entitlement control message of the primary

security system; the processor is to generate a substitutive entitlement control message as a replacement of the entitlement control message; and the access controlled data comprises the substitutive entitlement control message.

137. (Original)The conditional access server of claim 136, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

138. (Original)The conditional access server of claim 130, wherein the one or more communication interfaces are to receive a first entitlement control message containing a first control word and content scrambled by the first control word; the processor is to generate a second entitlement control message containing a second control word that is different from the first control word; and the conditional access server further comprises:

a transcrambler coupled to the one or more communication interfaces and the processor, the transcrambler to descramble the content using the first control word and rescramble the content using the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

139. (Original)The conditional access server of claim 138, further comprising:

a storage device coupled to the transcrambler, the storage device to store the content rescrambled by the second control word.

140. (Currently amended) A secondary conditional access client, comprising:

a communication interface to receive, from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system; and

a processor coupled to the communication interface, the processor to process the access controlled data,

wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust.

141. (Original)The client of claim 140, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

142. (Original)The client of claim 140, wherein the access controlled format protects access to data using a digital rights management system.

143. (Original)The client of claim 142, wherein the processor is to automatically determine whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data; the client further comprises:

a storage device;

a descrambler coupled to the processor and the storage device, in response to a determination to descramble the descrambler to descramble the portion of the media content for storing in the storage device, in response to a determination not to descramble the storage device to record the portion of the media content without descrambling.

144. (Original)The client of claim 142, wherein the communication interface is to send, to the conditional access server through a network connection, an entitlement control message containing a control word in an encrypted form; and the access controlled data comprises the control word.

145. (Original)The client of claim 144, further comprising:

a storage device;

a descrambler coupled to the processor and the storage device, the descrambler to descramble media content using the control word, the storage device to store the media content under protection of a digital rights management system.

146. (Previously Presented) The client of claim 140, further comprising:

a physical interface to receive a first entitlement control message for descrambling a portion of media content received from the primary security system; and

wherein the communication interface is to send the first entitlement control message to the conditional access server through a network connection.

REMARKS

35 U.S.C. § 103 Rejections

The Examiner has rejected claims 1-35, 37-40, 48-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132, 134-136, 137, 140-143 and 146 under 35 U.S.C. § 103(a) as being unpatentable over Grimes (U. S. Patent No. 7,036,011) in view of Simelius. The remaining claims have been rejected under §103(a) as being unpatentable over Grimes in view of Simelius and Candelore.

The primary rejection in the Office Action relies upon the combination of Grimes (US Pat 7,036,011) and Simelius (US Pat 7,493,291). The addition of Simelius allegedly corresponds to the claimed limitation that there are two independent authentication processes. Without agreeing with this interpretation of Simelius, Applicant has further amended the claims to make it clear that the two authentication processes are independent in that they use two different roots of trust that are independent. Simelius does not disclose this feature, and Grimes does not disclose this feature, and it is NOT intrinsic or inherent in either reference. Both systems (Grimes and Simelius) are still a single DRM system. There is NO bridge between two DRM systems in Grimes or Simelius. Hence, the rejection fails to establish a prima facie case for obviousness, and the addition of the third reference (Candelore, US Pat. 7,302,058) does not correct this failure to establish a prima facie case for obviousness. Therefore, the rejection should be withdrawn. Applicant will now provide a further discussion of Simelius.

The process of authentication of the child client by the parent client in Simelius happens when the parent client receives the public key of the child client (Simelius Column 15 – Row 3: Before enabling the child client 304 to access digital content, the…). The parent client must verify that the child client public key is chaining to the root of trust of the content server, or that

the child ID extracted from the public key is covered by the child vouchers owned by the parent. In both cases, the parent client is asked to validate the child client in the domain of the content server.

This demonstrates that Simelius doesn't consider two independent authentication processes, but defines a way for some devices (Parent client) to act as authentication proxy, voucher forwarder and content cacher for some other devices (Child client). The content server operates under the same root of trust as the parents and the child.

Simelius teaches a means to distribute vouchers and content to child devices that may or may not be in relation with the content server at the time of either transactions. It relies on parent devices to proxy the content server. While Simelius can have a lot of benefits if all the devices are compatible with the same security system, it does not offer the advantage of being able to reach devices that do not have the credentials required to be authenticated by the root of trust of the content server but could be reached through alternative security solutions.

In an embodiment, the present invention provides bridging between two security systems so that a secondary security system can securely present to a user a content previously secured by a primary security system. The present bridging process connects two independent authentication processes through a relationship between the two security systems.

For example, the primary security system can be a first conditional access (CA) server, servicing clients of the first CA server using a first authentication process. The secondary security system can be a second CA server, servicing clients of the second CA server using a second authentication process, which is independent of the first authentication process. The present invention provides a bridging service between a first CA client and a second CA server,

allowing the second CA server to receive content after being authenticated by the first CA server, and to present the content to a user pending a successful second authentication process.

In the prior art approaches, a client of a secondary CA server would need to subscribe to the primary CA server in order to receive services from the primary CA server. An advantage of the present bridging service allows a user to receive secured content from a primary system without directly subscribing to the primary system services. The service from the primary system can be received by the secondary system, which then presents it to the user.

Applicant submits that the combination of Grimes and Simelius fails to teach or disclose two security systems having two independent authentication processes that use two different and independent roots of trust. The two independent authentication processes are bridged through a client server relationship between the two security systems to allow the second security system to present to a user the encrypted content of the first security system.

Applicant, accordingly, respectfully requests withdrawal of the rejection of all claims.

The Examiner has rejected claims 36, 41-17, 52-56, 60, 61, 70, 75-81, 86-90, 94, 95, 104, 109-115, 120-124, 128, 129, 133, 137-139, 144 and 145 under 35 U.S.C. § 103(a) as being unpatentable over Grimes as applied to claims 32, 66, 100, 130 and 140 above, and further in view of Candelore (U. S. Patent No. 7,302,058). Candelore fails to disclose the limitations noted above and hence does not cure the deficiencies in the combination of Grimes and Simelius.

Applicant submits that these claims are dependent claims, thus should be allowable, at least for the reasons stated above.

CONCLUSION

Applicant respectfully submits that the present application is in condition for allowance.

If there are any additional charges, please charge them to our Deposit Account No. 02-2666. If a telephone conference would facilitate the prosecution of this application, the Examiner is invited to contact the undersigned at (408) 720-8300.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: March 2, 2010

James C. Scheller, Jr.
Reg. No. 31,195

Customer No. 08791
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

Electronic Patent Application Fee Transmittal	
Application Number:	11007116
Filing Date:	07-Dec-2004
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Filer:	James Scheller Jr./Connie Thayer
Attorney Docket Number:	6517P002
Filed as Large Entity	

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

IPR2025-00305
ASUS EX1002 Page 481

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	1801	1	810	810
		Total in USD ($)		**810**

Electronic Acknowledgement Receipt	
EFS ID:	7127482
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	08791
Filer:	James Scheller Jr./Connie Thayer
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	6517P002
Receipt Date:	02-MAR-2010
Filing Date:	07-DEC-2004
Time Stamp:	22:20:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$810
RAM confirmation Number	6248
Deposit Account	022666
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

IPR2025-00305
ASUS EX1002 Page 483

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	06517P002_RCE_transmittal.pdf	65203 772bb5350f0994c4464fe229f3be17bcc08d3996	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2		06517P002_amendment.pdf	1554538 573dea6975f7b9bde567801832a2fce519702d41	yes	47

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment Submitted/Entered with Filing of CPA/RCE	1	1
	Claims	2	43
	Applicant Arguments/Remarks Made in an Amendment	44	47

Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	29942 d8da3463df1814d4859ebd5f6390ee7921493b20	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1649683		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/007,116	12/07/2004	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	03/02/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 146	Minus	** 146	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 15	Minus	***15	= 0	X $ =		OR	X $220=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/Fennell A. Pearlie/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Atty. Docket No: 006517.P002 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Luc Vantalon	)	Examiner: Avery, Jeremiah L.
	)	
Application No.: 11/007,116	)	Art Unit: 2431
	)	
Filing Date: 12/7/2004	)	Conformation No. 9254
	)	
For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUMMARY OF INTERVIEW

Applicant thanks the examiner for the telephone interview on April 20, 2010.

During the interview applicant discussed the amended claims and the prior art, and the examiner indicated that he would reconsider these claims.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: April 20, 2010

James C. Scheller, Jr.
Reg. No. 31,195

IPR2025-00305
ASUS EX1002 Page 487

Electronic Acknowledgement Receipt	
EFS ID:	7453104
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	08791
Filer:	James Scheller Jr./David Baglietto
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	6517P002
Receipt Date:	20-APR-2010
Filing Date:	07-DEC-2004
Time Stamp:	18:13:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	006517_P002_Summary_of_Examiner_Interview.pdf	20609 74978e91c90c57416b19ee8f5ffb0556e3688ebd	no	1

Warnings:

Information:

IPR2025-00305
ASUS EX1002 Page 488

Total Files Size (in bytes):	20609

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

8791 7590 04/23/2010

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/23/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Interview Summary	Application No.	Applicant(s)	
	11/007,116	VANTALON ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Jeremiah Avery*. (3)*Eric Rindner*.

(2) *James C. Scheller, Jr. Reg. No. 31,195*. (4)*Luc Vantalon*.

Date of Interview: *20 April 2010*.

Type: a)☒ Telephonic b)☐ Video Conference
c)☐ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: *1*.

Identification of prior art discussed: *United States Patent No. 7,493,291 to Simelius*.

Agreement with respect to the claims f)☐ was reached. g)☒ was not reached. h)☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *The Applicants discussed the amended claim language and how it distinguishes itself from the prior art. The Examiner will consider the Applicants' remarks and conduct an updated search*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/Jeremiah Avery/ Examiner, Art Unit 2431	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

———

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IPR2025-00305
ASUS EX1002 Page 492

Atty. Docket No. 006517.P002 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Luc Vantalon	)	Examiner: Avery, Jeremiah L.
	)	
Application No. 11/007,116	)	Art Unit: 2431
	)	
Filed: 12/7/2004	)	
	)	Confirmation No. 9254
For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO INTERVIEW SUMMARY

Applicant thanks the examiner for the interview held on April 20, 2010 and notes that the examiner's interview summary correctly reflects the substance of the interview.

If any fees are required for this submission, please charge Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: May 10, 2010

James C. Scheller, Jr.
Reg. No. 31,195

1279 Oakmead Parkway
Sunnyvale, CA 94085
(408) 720-8300

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

May 10, 2010
Date of Deposit

David Baglietto
Name of Person Filing Correspondence

/ David Baglietto / 5/10/2010
Signature Date

IPR2025-00305
ASUS EX1002 Page 493

Electronic Acknowledgement Receipt

EFS ID:	7591297
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	08791
Filer:	James Scheller Jr./David Baglietto
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	6517P002
Receipt Date:	11-MAY-2010
Filing Date:	07-DEC-2004
Time Stamp:	16:44:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant summary of interview with examiner	006517_P002_Interview_Summary_Response.pdf	31267 2480a45896c6256da6c1762cede954f878994aaa	no	1

Warnings:	
Information:	

IPR2025-00305
ASUS EX1002 Page 494

Total Files Size (in bytes):	31267

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Substitute for Form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	11/007,116
				Filing Date	December 7, 2004
				First Named Inventor:	Luc Vantalon
				Art Unit	2431
				Examiner Name	Avery, Jeremiah L.
Sheet	**1**	**of**	**1**	Attorney Docket Number	6517P002

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (If known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-	7,546,641	06/09/2006	Robert et al.	
		US-				
		US-				
		US-				
		US-				

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08A (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.

Electronic Acknowledgement Receipt	
EFS ID:	8556789
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	08791
Filer:	James Scheller Jr./Harleen Bains
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	6517P002
Receipt Date:	04-OCT-2010
Filing Date:	07-DEC-2004
Time Stamp:	17:33:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		6517P002_IDS_and_1449.PDF	334725 b1ada75a065aa189dbf035f0e5e5f0d773cc545c	yes	3

IPR2025-00305
ASUS EX1002 Page 497

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Filed (SB/08)	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	334725	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IPR2025-00305
ASUS EX1002 Page 498

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:

Luc Vantalon, et al.

Application No.: 11/007,116

Filed: December 7, 2004

For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

Examiner: Avery, Jeremiah L.

Art Unit: 2431

Confirmation No.: 9254

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below.

H Bains 10/04/10

Harleen Bains ***Date***

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

INFORMATION DISCLOSURE STATEMENT

Sir:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 together with copies of the documents cited on that form, except for copies not required to be submitted (e.g., copies of U.S. patents and U.S. published patent applications need not be enclosed for applications filed after June 30, 2003). It is respectfully requested that the cited documents be considered and that the enclosed copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Pursuant to 37 C.F.R. § 1.97, this Information Disclosure Statement is being submitted under one of the following (as indicated by an "X" to the left of the appropriate paragraph):

__X__ 37 C.F.R. §1.97(b).

_____ 37 C.F.R. §1.97(c). If so, then enclosed with this Information Disclosure Statement is one of the following:

_____ A statement pursuant to 37 C.F.R. §1.97(e) or

_____ The Director is Authorized to charge our Deposit Acct. No. 02-2666 in the amount of $180.00 for the fee under 37 C.F.R. § 1.17(p).

_____ 37 C.F.R. §1.97(d). If so, then enclosed with this Information Disclosure Statement are the following:

(1) A statement pursuant to 37 C.F.R. §1.97(e); and

(2) Authorization to charge our Deposit Acct. No. 02-2666 in the amount of $180.00 for the fee under 37 C.F.R. §1.17(p) for submission of the Information Disclosure Statement.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: Oct. 4, 2010

James C. Scheller, Jr.
Reg. No. 31,195

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

Substitute for Form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	11/007,116
				Filing Date	December 7, 2004
				First Named Inventor:	Luc Vantalon
				Art Unit	2431
				Examiner Name	Avery, Jeremiah L.
Sheet	1	**of**	1	Attorney Docket Number	6517P002

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (If known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-	7,757,299	07-13-2010	Robert et al.	
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08A (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03.

Electronic Acknowledgement Receipt	
EFS ID:	11054238
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	Tatiana Rossin/Betty Scaletta
Filer Authorized By:	Tatiana Rossin
Attorney Docket Number:	6517P002
Receipt Date:	26-SEP-2011
Filing Date:	07-DEC-2004
Time Stamp:	21:35:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	6517P002_IDS_LTR_09-26-11.pdf	18042 54b30a2ff98316f3a6948e9fbe1ca58f07e837a0	no	2

Warnings:

Information:

IPR2025-00305
ASUS EX1002 Page 502

2	Information Disclosure Statement (IDS) Form (SB08)	6517P002_IDS_SB08_09-26-11.pdf	51787 35e79351403c1f92f6212e85209b9d83b5bea6b4	no	1

Warnings:	
Information:	
This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	69829

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	
Luc Vantalon	Examiner: Avery, Jeremiah L.
Application No.: 11/007,116	Art Unit: 2431
Filed: December 7, 2004	Confirmation No.: 9254
For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

INFORMATION DISCLOSURE STATEMENT

Sir:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08a together with copies of the documents cited on that form, except for copies not required to be submitted (e.g., copies of U.S. patents and U.S. published patent applications need not be enclosed for applications filed after June 30, 2003). It is respectfully requested that the cited documents be considered and that the enclosed copy of Information Disclosure Citation Form PTO-1449 or PTO/SB/08a be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

09-26-2011
Date of Deposit

/Betty Scaletta/
Betty Scaletta

IPR2025-00305
ASUS EX1002 Page 504

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Pursuant to 37 C.F.R. § 1.97, this Information Disclosure Statement is being submitted under one of the following (as indicated by an "X" to the left of the appropriate paragraph):

__X__ 37 C.F.R. §1.97(b).

_____ 37 C.F.R. §1.97(c). If so, then enclosed with this Information Disclosure Statement is one of the following:

____ A statement pursuant to 37 C.F.R. §1.97(e) or

____ The Director is Authorized to charge our Deposit Acct. No. 02-2666 in the amount of $180.00 for the fee under 37 C.F.R. § 1.17(p).

_____ 37 C.F.R. §1.97(d). If so, then enclosed with this Information Disclosure Statement are the following:

(1) A statement pursuant to 37 C.F.R. §1.97(e); and

(2) Authorization to charge our Deposit Acct. No. 02-2666 in the amount of $180.00 for the fee under 37 C.F.R. §1.17(p) for submission of the Information Disclosure Statement.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: September 26, 2011 /Tatiana Rossin/
Tatiana Rossin
Reg. No. 56,833

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

Customer No.: 08791

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

8791 7590 01/03/2012

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
01/03/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/007,116	VANTALON ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-146* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-146* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *07 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

I. Claims 1-146 have been examined.

II. Responses to Applicant's Remarks have been given.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/02/10 has been entered.

Response to Arguments

2. With regards to the Applicant's arguments pertaining to the newly-added amended claim language of "a second root of trust independent of and different than the first root of trust", said arguments are rendered moot in view of the new grounds of rejection set forth below.

3. With regards to the Applicant's argument that "Candelore fails to disclose the limitations noted above and hence does not cure the deficiencies in Grimes and Simelius", the Examiner asserts that Candelore significantly discloses the parts of the claimed invention pertaining to the "control words", as cited below.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 10-18 and 62-95 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claims 10, 62, 66 and 82 are directed towards "a machine readable medium containing executable computer program instructions…". Amendments to the claims indicating that said "medium" is non-transitory" would render the claims statutory. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-35, 37-40, 4-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132, 134-136, 137, 140-143 and 146 are rejected under 35 U.S.C. 103(a) as being unpatentable over by United States Patent No. 7,036,011 to Grimes et al., hereinafter Grimes, and further in view of United States

Patent No. 7,493,291 to Simelius, hereinafter Simelius and further in view of United States Patent No. 6,961,858 to Fransdonk, hereinafter Fransdonk.

5. Regarding claim 1, Grimes teaches a method to control a presentation of content, the method comprising:

receiving a representation of content from a first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access (column 2, lines 1-31, “content is encrypted with an encryption key”);

presenting the content, at a user's request, through a second conditional access server which is coupled to the first conditional access server (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

wherein the presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”);

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content (column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

6. Grimes teaches the claimed invention, as cited above. However, Grimes does not teach the claim language with regards to "wherein the first conditional access server authenticates client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates client devices of the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process". Simelius teaches said claim language, as cited below.

7. Regarding claim 1, Simelius teaches wherein the first conditional access server authenticates client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates client devices of the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, "second parent client" and lines 60-65, "first parent client", column 14, lines 18-37 and column 15, lines 42-53).

8. The motivation to combine would be "This provides a solution for more flexible use of digital content across a plurality of devices, while the use cannot be freely copied." (*Simelius* – column 7, lines 63-65).

9. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Simelius with the teachings

of Grimes so that “the exchange of rights to access digital content between devices will facilitate a user-friendly environment in any situation for consuming the digital content” (*Simelius* – column 7, lines 65-67).

10. Further, the claim language within independent claims 10, 28 and 62 which were rejected in view of Simelius is analogous to the claim language set forth within claim 1 and thus the motivation and obviousness to combine for independent claim 1 will also pertain to independent claims 10, 28 and 62.

11. Grimes and Simelius teach the claimed invention, as cited above. However, they do not disclose the claimed invention with regards to “wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust". Fransdonk teaches this feature, as cited below.

12. Fransdonk teaches wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust via Figures 16 and 17 and column 34, lines 33-59, “logically separating user authentication functionality from content security (i.e., copy-protected device authentication)" and "verification of two separate certificates, namely a first user device certificate for user authentication and a second secure copy-protected device certificate for content security authentication" and lines 63-67 and column 35, lines 1-32 and 37-51.

13. The motivation to combine would be that by "moving security functionality, implemented by a conditional access agent 28 in the manner described below, away from an end user device (e.g., a secure device 46) increases security as this

functionality is located outside the reach of hackers at a content destination 22" (*Franksdonk* – column 22, lines 17-24).

14. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Fransdonk with the teachings of Grimes and Simelius in order to provide a more secure environment for accessing requested content by appropriately authenticated users.

15. Further, the claim language within independent claims 10, 19, 23, 28, 32, 48, 62, 66, 82, 96, 100, 116, 130 and 140 is analogous to the claim language set forth within claim 1, thus the motivation and obviousness to combine for claim 1 (in view of Fransdonk) will also pertain to claims 10, 19, 23, 28, 32, 48, 62, 66, 82, 96, 100, 116, 130 and 140.

16. Regarding claim 2, Grimes teaches wherein the content is presented by a network client of the second conditional access server using the second set of cryptographic keys (column 4, lines 20-28, column 5, lines 50-56, column 6, lines 35-52, "encrypting and transmitting the encryption key 98" and column 7, lines 30-51).

17. Regarding claim 3, Grimes teaches wherein the first conditional access server provides the second conditional access server the first set of cryptographic keys for authorized use (column 5, lines 50-56, column 6, lines 35-52, column 7, lines 11-29, "if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content", column 8, lines 51-62 and column 9, lines 38-60).

18. Regarding claim 4, Grimes teaches wherein the user's request is after the first conditional access server provides at least a portion of the content; and the portion of the content is presented in response to the user's request (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

19. Regarding claims 5 and 14, Grimes teaches wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the network client is a digital rights management client (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

20. Regarding claims 6 and 14, Grimes teaches wherein the second conditional access server authorizes the network client to use the content through the digital rights management system in accordance with authorization to use received from the first conditional access server (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

21. Regarding claims 7 and 20, Grimes teaches wherein the second conditional access server translates authorization to access the content from authorization received from the first conditional access server to authorization for the network client (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

22. Regarding claims 8, 17 and 27, Grimes teaches wherein the second set of cryptographic keys consists one key (column 2, lines 1-31, “content is encrypted with an encryption key”).

23. Regarding claim 9, Grimes teaches wherein the second conditional access server acts as a primary conditional access server to another secondary conditional access server (column 7, lines 18-23, “the DRM server 58 or other server at the NOC 12”, column 8, lines 16-31, “third-party website server” and column 9, lines 3-11).

24. Regarding claim 10, Grimes discloses a machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content, the method comprising:

receiving, at a second conditional access server, a first set of cryptographic keys from a first conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

authorizing a client of the second conditional access server to present the content in accordance with authorization the second conditional access server received from the first conditional access server (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”);

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content (column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

25. Regarding claim 10, Simelius discloses wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates clients of the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

26. Regarding claim 11, Grimes discloses wherein the method further comprises: recording a representation of the content in an encrypted form in response to a message from the first conditional access server (column 2, lines 10-21, column 6, lines 35-52, column 7, lines 30-51, column 8, lines 16-31 and 51-62, column 9, lines 3-20, column 10, lines 19-29 and 37-46 and column 11, lines 26-47).

27. Regarding claim 12, Grimes discloses wherein the client sends a request, through a network connection to the second conditional access server, for authorization

to present the content after the first conditional access server provides at least a portion of the content which is recorded; the second conditional access server obtains authorization from the first conditional access server, after the first conditional access server provides the portion of the content, for said authorizing (column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

28. Regarding claim 13, Grimes discloses wherein the method further comprises: translating authorization to access the content from authorization received from the first conditional access server to authorization for the client (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

29. Regarding claim 16, Grimes discloses wherein the first conditional access server provides authorization to the second conditional access server according to an identity of the second conditional access server; the second conditional access server provides authorization to the client according to an identity of the client (column 3, lines 29-41, column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18);

the first conditional access server is not aware of an identity of the client (column 7, lines 40-51, “generating a digital certificate 84 may be performed by the third-party website server (e.g., when the user orders content from a third-party website)").

30. Regarding claim 18, Grimes discloses wherein the second conditional access server is a server of a further secondary conditional access server and acts as a primary conditional access server with respect to the further secondary conditional access server (column 7, lines 18-23, “the DRM server 58 or other server at the NOC 12”, column 8, lines 16-31, “third-party website server” and column 9, lines 3-11).

31. Regarding claims 19 and 23, Grimes discloses a secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

a communication interface, the communication interface to receive a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys (column 2, lines 10-39, “computer-readable medium further comprises instructions for requesting the encryption key from a digital rights management (DRM) server using a digital certificate”, column 4, lines 29-49, column 5, lines 53-65, column 7, lines 11-29 and column 13, lines 4-18);

a controller coupled to the communication interface, the controller to authorize a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server; wherein the secondary conditional access server uses a

second set of cryptographic keys to protect the content from unauthorized access in presenting the content (column 7, lines 11-29, "if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content", column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

32. Grimes significantly discloses the claimed invention, as cited above. However, Grimes does not substantially disclose the claim language pertaining to "wherein the primary conditional access server authenticates clients of the primary conditional access server through a first authentication process and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process". Simelius discloses said claim language, as cited below.

33. Regarding claims 19 and 23, Simelius discloses wherein the primary conditional access server authenticates clients of the primary conditional access server through a first authentication process using a first root of trust and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, "second parent client" and lines 60-65, "first parent client", column 14, lines 18-37 and column 15, lines 42-53).

34. The motivation to combine would be "This provides a solution for more flexible use of digital content across a plurality of devices, while the use cannot be freely copied." (*Simelius* – column 7, lines 63-65).

35. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Simelius with the teachings of Grimes so that "the exchange of rights to access digital content between devices will facilitate a user-friendly environment in any situation for consuming the digital content" (*Simelius* – column 7, lines 65-67).

36. Regarding claim 21, Grimes discloses wherein the second set of cryptographic keys comprises a key of a digital rights management system; the client comprises a digital rights management client; the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

37. Regarding claims 22 and 26, Grimes discloses wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of the client (column 3, lines 29-41, column 7, lines 11-29, "if the ordered content is PPV

content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content", column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18);

the primary conditional access server is not aware of an identity of the client (column 7, lines 40-51, "generating a digital certificate 84 may be performed by the third-party website server (e.g., when the user orders content from a third-party website)").

38. Regarding claim 24, Grimes discloses means for recording a representation of the content in an encrypted form in response to a message from the primary conditional access server. wherein the client sends a request, through a network connection to the secondary conditional access server, for authorization to present the content after the primary conditional access server provides at least a portion of the content which is recorded; the secondary conditional access server obtains authorization from the primary conditional access server, after the primary conditional access server provides the portion of the content, for authorizing the client to present the content (column 7, lines 7-29, "if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content", column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

39. Regarding claim 25, Grimes discloses means for translating authorization to access the content from authorization received from the primary conditional access server to authorization for the client. wherein the second set of cryptographic keys

comprises a key of a digital rights management system; the client comprises a digital rights management client; wherein the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

40. Regarding claims 28 and 62, Grimes teaches a method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component; broadcasting the media component from a first conditional access server; receiving a client request to use the media component from a client through a second conditional access server after said broadcasting; responding to the client request from the client of the second conditional access server (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

41. Regarding claims 28 and 62, Simelius teaches wherein the first conditional access server authenticates clients of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates clients of the second conditional access server authenticates clients of the second conditional access server through a second authentication process

which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

42. Regarding claims 29, 63 and 97, Grimes teaches broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request (column 7, lines 7-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

43. Regarding claims 30, 64 and 98, Grimes teaches wherein the client is not authorized to use the portion of the media content before the second entitlement management message (column 11, lines 3-19, "validation refused" and column 13, lines 4-18, "the hardware profile will not match the user machine 40 of client 18 if the user has made an unauthorized transfer of the client software 43").

44. Regarding claims 31, 65 and 99, Grimes teaches wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously (column 3, lines 61-67, column 4, lines 1-9, “this stored or personal content 28 may be kept on a user machine hard-drive or other storage medium” and 42-59 and column 5, lines 1-18).

45. Regarding claims 32, 66, 100 and 130, Grimes teaches a method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

processing the security messages on the conditional access server (column 2, lines 1-31, column 5, lines 19-29 and 50-56, column 6, lines 14-34 and column 9, lines 26-37);

transmitting, from the conditional access server to a secondary conditional access client through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from the security messages (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

46. Grimes significantly teaches the claim language, as cited above, but it does not substantially teach the claim language pertaining to “wherein the primary security system authenticates clients of the primary security system through a first authentication process and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process”. Simelius teaches said claim language, as cited below.

47. Regarding claims 32, 66, 100 and 130, Simelius teaches wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication

process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

48. The motivation to combine would be “This provides a solution for more flexible use of digital content across a plurality of devices, while the use cannot be freely copied.” (*Simelius* – column 7, lines 63-65).

49. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Simelius with the teachings of Grimes so that “the exchange of rights to access digital content between devices will facilitate a user-friendly environment in any situation for consuming the digital content” (*Simelius* – column 7, lines 65-67).

50. The claim language within claims 48, 82, 96, 116 and 140 are analogous to the claim language above; thus the motivation and obviousness to combine for claims 32, 66, 100 and 130 will also pertain to claims 48, 82, 96, 116 and 140.

51. Regarding claims 33, 67 and 101, Grimes teaches wherein the security messages comprise entitlement management messages;

the conditional access server has a user key representing a subscriber of the primary security system (column 6, lines 65-67, column 7, lines 1-29 and column 8, lines 43-50);

said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system (column 9, lines 24-60).

52. Regarding claims 34, 68 and 102, Grimes teaches wherein the access controlled data is protected using a digital rights management system (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

53. Regarding claims 35, 69, 103 and 132, Grimes teaches wherein rights to the access controlled data are at least partially derived from the entitlement management messages (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

54. Regarding claims 38, 72, 106 and 134, Grimes teaches receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system (column 12, lines 26-61 and column 13, lines 19-25 and 28-30); descrambling the scrambled content according to the entitlement control message; wherein the access controlled data comprises a result of descrambling the scrambled content (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

55. Regarding claims 39, 73, 107 and 135, Grimes teaches storing, at the conditional access server, the content in an encrypted form; wherein the access controlled data is provided in response to a request from the secondary conditional access client (column 2, lines 10-21, column 6, lines 35-52, column 7, lines 30-51, column 8, lines 16-31 and 51-62, column 9, lines 3-20, column 10, lines 19-29 and 37-46 and column 11, lines 26-47).

56. Regarding claims 40, 74, 108, 136, Grimes teaches receiving, at the conditional access server, an entitlement control message of the primary security system; processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message; wherein the access controlled data comprises the substitutive entitlement control message (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

57. Regarding claims 48, 82 and 116, Grimes teaches a method to process media content provided by a primary security system, the method comprising:
receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

58. Regarding claims 48, 82 and 116, Simelius teaches wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines

50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

59. Regarding claims 49, 83, 117 and 141, Grimes teaches wherein the security message is an entitlement message; wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system (column 7, lines 40-51, “generating a digital certificate 84 may be performed by the third-party website server (e.g., when the user orders content from a third-party website)", column 11, lines 3-19, "validation refused" and column 13, lines 4-18, "the hardware profile will not match the user machine 40 of client 18 if the user has made an unauthorized transfer of the client software 43").

60. Regarding claims 50, 84, 118 and 142, Grimes teaches wherein the access controlled format protects access to data using a digital rights management system (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

61. Regarding claims 51, 85 and 119, Grimes teaches automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data (column 12, lines 26-61 and column 13, lines 19-25 and 28-30);

descrambling and recording the portion of the media content in response to a determination to descramble (column 12, lines 62-67 and column 13, lines 1-3 and 25-28);

recording the portion of the media content without descrambling in response to a determination not to descramble (column 12, lines 26-61 and column 13, lines 19-25 and 28-30).

62. Regarding claims 57, 91 and 125, Grimes teaches wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

63. Regarding claims 58, 92 and 126, Grimes teaches receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

64. Regarding claims 59, 93 and 127, Grimes teaches wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; the method further comprises: storing the second entitlement control message with the portion of the media content (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

65. Regarding claim 96, Grimes discloses a primary security system to provide conditional access, the method comprising:

means for broadcasting a first entitlement management message for a subscriber to request caching of a media component; broadcasting the media component from a first conditional access server; receiving a client request to use the media component from a client of a second conditional access server after said broadcasting; responding to the client request from the client of the second conditional access server (column 3, lines 29-41, column 6, lines 35-52, column 7, lines 11-29, column 8, lines 32-50, column 9, lines 24-37 and 61-67 and column 10, lines 1-8 and 22-33).

66. Regarding claim 96, Simelius discloses wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

67. Regarding claim 131, Grimes discloses wherein the security messages comprise entitlement management messages; the access controlled data is protected using a digital rights management system (column 2, lines 1-39, column 4, lines 23-28 and 42-49, column 5, lines 19-39 and 50-65, column6, lines 14-22, column 7, lines 11-55, column 8, lines 5-31, column 9, lines 38-60, column 10, lines 10-29, 34-52 and 59-67, column 11, lines 1-11 and 26-51 and column 13, lines 4-18).

68. Regarding claim 140, Grimes discloses a secondary conditional access client, comprising:

a communication interface to receive, from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system;

a processor coupled to the communication interface, the processor to process the access controlled data (column 7, lines 11-29, “only those clients 18 that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate”).

69. Regarding claim 140, Simelius discloses wherein the primary security system authenticates clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process (column 7, lines 29-62, column 8, lines 50-67, column 9, lines 1-4, column 13, lines 38-50, “second parent client” and lines 60-65, “first parent client”, column 14, lines 18-37 and column 15, lines 42-53).

70. Regarding claim 143, Grimes discloses wherein the processor is to automatically determine whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data (column 12, lines 26-61 and column 13, lines 19-25 and 28-30);

the client further comprises:

a storage device; a descrambler coupled to the processor and the storage device, in response to a determination to descramble the descrambler to descramble the portion of the media content for storing in the storage device, in response to a determination not to descramble the storage device to record the portion of the media content without descrambling (column 12, lines 62-67 and column 13, lines 1-3 and 25-28).

71. Regarding claim 146, Grimes discloses a physical interface to receive a first entitlement control message for descrambling a portion of media content received from the primary security system (column 12, lines 62-67 and column 13, lines 1-3 and 25-28);

and wherein the communication interface is to send the first entitlement control message to the conditional access server through a network connection (column 3, lines 29-41, column 7, lines 11-29, “if the ordered content is PPV content or subscription content, or is otherwise restricted content, a digital certificate may be generated for the content and the content may be encrypted so that only clients 18 that receive the digital certificate can access the content”, column 8, lines 51-62, column 9, lines 38-60 and column 13, lines 4-18).

72. Claims 36, 41-47, 52-56, 60, 61, 70, 75-81, 86-90, 94, 95, 104, 109-115, 120-124, 128, 129, 133, 137-139, 144 and 145 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grimes, Simelius and Fransdonk, as applied to claims 32, 66, 100, 130 and 140 above, and further in view of United States Patent No. 7,302,058 to Candelore, hereinafter Candelore.

73. Grimes, Simelius and Fransdonk significantly teach the claimed invention, as cited above. However, Grimes, Simelius and Fransdonk do not substantially teach the claim language in the following claims pertaining to "control words". Candelore teaches said claim language, as cited below.

74. The motivation to combine would be that "the control word is only decrypted in descrambler IC 440 that actually uses the control word, therefore, the control word is never exposed, and cannot be obtained by hackers". (*Candelore* – column 6, lines 42-49).

75. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Candelore with the teachings of Grimes, Simelius and Fransdonk so that "Local Access control can be performed by the Insecure Processor because the critical 'secure' function is isolated in the Descrambler IC" (*Candelore* – column 10, lines 48-54).

76. Regarding claims 36, 70, 104 and 133, Candelore teaches receiving, at the conditional access server, an entitlement control message of the primary security system (column 3, lines 61-67, column 4, lines 1-14 and 55-67 and column 5, lines 1-3 and 20-26);

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system (column 5, lines 20-26 and column 6, lines 11-31 and 42-51);

wherein the access controlled data comprises the control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines

11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

77. Regarding claims 37, 71 and 105, Candelore teaches wherein the access controlled data comprises a decrypted version of the entitlement control message (column 4, lines 6-14, column 6, lines 32-49 and column 7, lines 25-41).

78. Regarding claims 41, 75, 109 and 137, Candelore teaches wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server (column 3, lines 15-23, column 6, lines 11-31, “encrypts the CWs in encryption block 414 with keys that are unique to transport descrambler integrated circuit (IC) 440” and column 7, lines 54-62).

79. Regarding claims 42, 76 and 110, Candelore teaches wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system (column 4, lines 9-13 and column 6, lines 11-20 and 42-49).

80. Regarding claims 43, 77 and 111, Candelore teaches wherein the entitlement control message and the substitutive entitlement control message have a same control word (Figure 2, element 416 and Figure 3, elements 41, 44 and 45, column 3, lines 15-23, column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

81. Regarding claims 44, 78 and 112, Candelore teaches wherein the entitlement control message has a first control word (Figure 2, element 416, Figure 3, elements 41,

44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41);

the substitutive entitlement control message has a second control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

the first and second control words are different (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61).

82. Regarding claims 45, 79 and 113, Candelore teaches wherein the access controlled data further comprises the first and second control words (Figure 6, "encrypted control word A" and "encrypted control word B" and column 7, lines 42-61).

83. Regarding claims 46, 80, 114 and 138, Candelore teaches receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word (column 3, lines 15-24 and column 6, lines 14-17 and 60-63);

generating a second entitlement control message containing a second control word that is different from the first control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

descrambling the content using the first control word and rescrambling the content by the second control word (column 6, lines 11-20, column 7, lines 54-67 and column 8, lines 1-23);

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message (column 5, lines 55-65).

84. Regarding claims 47, 81 and 115, Candelore teaches storing, at the conditional access server, the content rescrambled by the second control word (column 5, lines 55-65);

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client (column 5, lines 55-65 and column 6, lines 1-10).

85. Regarding claims 52, 86, 120 and 144, Candelore teaches sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form (column 5, lines 20-26 and column 6, lines 11-31 and 42-51);

wherein the access controlled data comprises the control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, and column 7, lines 25-41).

86. Regarding claims 53, 87 and 121, Candelore teaches descrambling media content using the control word (Figure 2, element 416, Figure 3, elements 41, 44 and 45 and Figure 6, column 3, lines 15-23, column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41);

storing the media content in a storage under protection of a digital rights management system (column 6, lines 11-31 and 42-51).

87. Regarding claims 54, 88 and 122, Candelore teaches descrambling media content using the control word; and rendering the media content for presentation (column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

88. Regarding claims 55, 89 and 123, Candelore teaches retrieving the entitlement control message from a storage device (column 6, lines 11-31 and 42-51);
wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client (column 3, lines 61-67, column 4, lines 1-14 and 55-67 and column 5, lines 1-3 and 20-26).

89. Regarding claims 56, 90 and 124, Candelore teaches wherein the access controlled data comprises a decrypted version of the entitlement control message (column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

90. Regarding claims 60, 94 and 128, Candelore teaches wherein both the first and the second entitlement control messages contain a same control word (Figure 2, element 416 and Figure 3, elements 41, 44 and 45, column 3, lines 15-23, column 6,

lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41);

the second entitlement control message is encrypted to be decrypted using a key of the conditional access server (column 4, lines 6-14, column 6, lines 32-49 and column 7, lines 25-41).

91. Regarding claims 61, 95 and 129, Candelore teaches wherein the first entitlement control message contains a first control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 3, lines 15-24 and column 6, lines 14-17 and 60-63);

the second entitlement control message contains a second control word (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

the first and second control words are different (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

the access controlled data further comprises the first and second control words (Figure 6, "encrypted control word A" and "encrypted control word B", column 7, lines 42-61);

the method further comprises: descrambling the content using the first control word and rescrambling the content using the second control word (column 5, lines 55-65).

92. Regarding claim 139, Candelore discloses a storage device coupled to the transcrambler, the storage device to store the content rescrambled by the second control word (column 5, lines 55-65).

93. Regarding claim 145, Candelore discloses a storage device;

a descrambler coupled to the processor and the storage device, the descrambler to descramble media content using the control word, the storage device to store the media content under protection of a digital rights management system (column 6, lines 11-63, “conditional access unit 401 will decrypt the control words and use the clear control words to descramble the program content” and column 7, lines 25-41).

Conclusion

94. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

95. The following United States Patents and Patent Application Publication are cited to further show the state of the art with respect to the access control of content, such as:

United States Patent No. 7,127,619 to Unger et al., which is cited to show the decoding and decryption of partially encrypted information.

United States Patent No. 7,171,558 to Mourad et al., which is cited to show transparent digital rights management for extendible content viewers.

United States Patent No. 7,177,429 to Moskowitz et al., which is cited to show system and methods for permitting open access to data objects and for securing data within the data objects.

United States Patent No. 7,292,692 to Bonan et al., which is cited to show content scrambling with minimal impact on legacy devices.

United States Patent No. 7,316,032 to Tayebi et al., which is cited to show a method for allowing a customer to preview, acquire and/or pay for the information and a system therefor.

United States Patent No. 7,336,784 to Zuili which is cited to show a multimedia decoder method and system with authentication and enhanced digital rights management (DRM) where each received signal is unique and where the missing signal is cached inside the storage memory of each receiver.

United States Patent Application Publication No. US 2004/0196842 to Dobbins which is cited to show a method and system for according preferred transport based on node identification.

United States Patent No. 7,296,154 to Evans et al., which is cited to show secure media path methods, systems and architectures.j

United States Patent No. 7,174021 to Krishnaswamy et al., which is cited to show systems and methods for providing secure server key operations.

96. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

97. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

98. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431

/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/007,116	Applicant(s)/Patent Under Reexamination VANTALON ET AL.	
	Examiner JEREMIAH AVERY	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,961,858	11-2005	Fransdonk, Robert W.	726/29
*	B	US-7,036,011	04-2006	Grimes et al.	713/156
*	C	US-7,493,291	02-2009	Simelius, Kim	705/59
*	D	US-7,302,058	11-2007	Candelore, Brant L.	380/200
*	E	US-7,127,619	10-2006	Unger et al.	713/193
*	F	US-7,171,588	01-2007	Friedman et al.	714/38.12
*	G	US-7,177,429	02-2007	Moskowitz et al.	380/252
*	H	US-7,292,692	11-2007	Bonan et al.	380/212
*	I	US-7,316,032	01-2008	Tayebi et al.	705/51
*	J	US-7,336,784	02-2008	Zuili, Patrick	380/200
*	K	US-2004/0196842	10-2004	Dobbins, Kurt A.	370/389
*	L	US-7,296,154	11-2007	Evans et al.	713/169
*	M	US-7,174,021	02-2007	Krishnaswamy et al.	380/277

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Substitute for Form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	11/007,116
				Filing Date	December 7, 2004
				First Named Inventor:	Luc Vantalon
				Art Unit	2431
				Examiner Name	Avery, Jeremiah L.
Sheet	1	**of**	1	Attorney Docket Number	6517P002

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (If known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-	7,757,299	07-13-2010	Robert et al.	
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	12/22/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SENT FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Based on Form PTO/SB/08A (08-03) as modified by BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP on 09/10/03

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/28/2011								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/28/2011								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	46	✓								
	47	✓								
	48	✓								
	49	✓								
	50	✓								
	51	✓								
	52	✓								
	53	✓								
	54	✓								
	55	✓								
	56	✓								
	57	✓								
	58	✓								
	59	✓								
	60	✓								
	61	✓								
	62	✓								
	63	✓								
	64	✓								
	65	✓								
	66	✓								
	67	✓								
	68	✓								
	69	✓								
	70	✓								
	71	✓								
	72	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/28/2011								
	73	✓								
	74	✓								
	75	✓								
	76	✓								
	77	✓								
	78	✓								
	79	✓								
	80	✓								
	81	✓								
	82	✓								
	83	✓								
	84	✓								
	85	✓								
	86	✓								
	87	✓								
	88	✓								
	89	✓								
	90	✓								
	91	✓								
	92	✓								
	93	✓								
	94	✓								
	95	✓								
	96	✓								
	97	✓								
	98	✓								
	99	✓								
	100	✓								
	101	✓								
	102	✓								
	103	✓								
	104	✓								
	105	✓								
	106	✓								
	107	✓								
	108	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/28/2011								
	109	✓								
	110	✓								
	111	✓								
	112	✓								
	113	✓								
	114	✓								
	115	✓								
	116	✓								
	117	✓								
	118	✓								
	119	✓								
	120	✓								
	121	✓								
	122	✓								
	123	✓								
	124	✓								
	125	✓								
	126	✓								
	127	✓								
	128	✓								
	129	✓								
	130	✓								
	131	✓								
	132	✓								
	133	✓								
	134	✓								
	135	✓								
	136	✓								
	137	✓								
	138	✓								
	139	✓								
	140	✓								
	141	✓								
	142	✓								
	143	✓								
	144	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/28/2011								
	145	✓								
	146	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

SEARCHED			
Class	Subclass	Date	Examiner
none	none	12/20/2011	JLA

SEARCH NOTES		
Search Notes	Date	Examiner
Updated EAST Search	12/20/2011	JLA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
none	none	12/20/2011	JLA

Substitute for Form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	11/007,116
				Filing Date	December 7, 2004
				First Named Inventor:	Luc Vantalon
				Art Unit	2431
				Examiner Name	Avery, Jeremiah L.
Sheet	**1**	**of**	**1**	Attorney Docket Number	6517P002

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (If known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-	7,546,641	06/09/2006	Robert et al.	
		US-				
		US-				
		US-				
		US-				

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]

Examiner Signature	/Jeremiah Avery/	Date Considered	12/22/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1236	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:08
L2	1195	l1 and ((first or primary) or (second$3 or other or next or another) with ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) with (authentic$ or verify$ or verification)))	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:12
L3	158	l2 and (access near server)	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:13
L4	109	l3 and (server same (($2crypt $ or $2cipher) near key))	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:19
L5	83	l4 and ($2authoris$ or $2authoriz$)	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:24
L6	64	l5 and (($2authoris$ or $2authoriz$) with access$)	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:25
S1	990	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT	OR	ON	2009/03/26 19:43

S2	873	S1 and server	US-PGPUB; USPAT	OR	ON	2009/03/26 19:48
S3	522	S2 and unauthori$	US-PGPUB; USPAT	OR	ON	2009/03/26 19:49
S4	447	S3 and (authoris$ or authoriz$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:49
S5	433	S4 and (ID or identit$ or identif$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:50
S6	420	S5 and ((first or primary) or (second$ or other) near server)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:50
S7	402	S6 and (broadcast$ or transmit$ or transmission or send$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:52
S8	395	S7 and ((broadcast$ or transmit$ or transmission or send$) same (media or audio or video or stream or content or data or information))	US-PGPUB; USPAT	OR	ON	2009/03/26 19:52
S9	317	S8 and (play$ or playback)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:53
S10	150	S9 and (subscribe$ or subscript$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:54
S11	39	S10 and $2scrambl$	US-PGPUB; USPAT	OR	ON	2009/03/26 19:54
S12	7	S11 and (control$5 near word)	US-PGPUB; USPAT	OR	ON	2009/03/26 20:00
S13	1058	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S14	932	S13 and server	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01

S15	556	S14 and unauthori$	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S16	477	S15 and (authoris$ or authoriz$)	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S17	461	S16 and (ID or identit$ or identif$)	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S18	448	S17 and ((first or primary) or (second$ or other) near server)	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S19	448	S18 and ((first or primary) or (second$ or other) near (authentic$ or verify$ or verification))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:02
S20	448	S19 and ((first or primary) or (second$ or other or next) near ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:06
S21	0	S20 and (((first or primary) or (second$ or other or next) near (access near server)) near ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:08
S22	7	S20 and (((first or primary) or (second$ or other or next) near (access near server)) same ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:09
S23	7	S20 and (((first or primary) or (second$ or other or next) near server) same ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:22

S24	0	S20 and (((first or primary) or (second$ or other or next) near server) near ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:23
S25	55	S20 and (((first or primary) or (second$ or other or next) near server) near (authentic$ or verify$ or verification))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:24
S26	11	S25 and ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:25

12/20/2011 6:05:39 PM
C:\Documents and Settings\javery\My Documents\EAST\Workspaces\11007116.wsp

IPR2025-00305
ASUS EX1002 Page 554

Attorney's Docket No. 6517P002 Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Luc Vantalon Application No.: 11/007,116 Filed: December 7, 2004 For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	Examiner: Avery, Jeremiah L. Art Unit: 2431 Confirmation No.: 9254 **CERTIFICATE OF TRANSMISSION** I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below. /Betty Scaletta/ 05-01-2012 ***Betty Scaletta*** ***Date***

Filed via EFS-Web
Commissioner for Patents
Alexandria, VA 22313-1450

AMENDMENT

Sir:

In response to the Office Action mailed January 3, 2012, applicant submits the following amendment and remarks for consideration.

IN THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application.

Please amend the claims as follows:

1. (Currently Amended) A method to control a presentation of content, the method comprising:

receiving a representation of content from a first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access in a first security domain; and

presenting the content, at a user's request, through a second conditional access server which is coupled to the first conditional access server;

wherein the presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively;

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain; and

wherein the first conditional access server authenticates the second conditional access server as one of client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.

2. (Original) The method of claim 1, wherein the content is presented by a network client of the second conditional access server using the second set of cryptographic keys.

3. (Original) The method of claim 2, wherein the first conditional access server provides the second conditional access server the first set of cryptographic keys for authorized use.

4. (Original) The method of claim 3, wherein the user's request is after the first conditional access server provides at least a portion of the content; and the portion of the content is presented in response to the user's request.

5. (Original) The method of claim 2, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the network client is a digital rights management client.

6. (Original) The method of claim 5, wherein the second conditional access server authorizes the network client to use the content through the digital rights management system in accordance with authorization to use received from the first conditional access server.

7. (Original) The method of claim 1, wherein the second conditional access server translates authorization to access the content from authorization received from the first conditional access server to authorization for the network client.

8. (Original) The method of claim 1, wherein the second set of cryptographic keys consists one key.

9. (Original) The method of claim 1, wherein the second conditional access server acts as a primary conditional access server to another secondary conditional access server.

10. (Currently Amended) A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content, the method comprising:

receiving, at a second conditional access server, a first set of cryptographic keys from a first conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys in a first security domain; and

authorizing a client of the second conditional access server to present the content in accordance with authorization the second conditional access server received from the first conditional access server;

wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain; and

wherein the first conditional access server authenticates the second conditional access server as one of clients of the first conditional access server through a first authentication process using a first root of trust and the second conditional access

IPR2025-00305
ASUS EX1002 Page 558

server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.

11. (Original) The medium of claim 10, wherein the method further comprises:

recording a representation of the content in an encrypted form in response to a message from the first conditional access server.

12. (Original) The medium of claim 11, wherein the client sends a request, through a network connection to the second conditional access server, for authorization to present the content after the first conditional access server provides at least a portion of the content which is recorded; and the second conditional access server obtains authorization from the first conditional access server, after the first conditional access server provides the portion of the content, for said authorizing.

13. (Original) The medium of claim 10, wherein the method further comprises:

translating authorization to access the content from authorization received from the first conditional access server to authorization for the client.

14. (Original) The medium of claim 13, wherein the second set of cryptographic keys comprises a key of a digital rights management system; and the client comprises a digital rights management client.

15. (Original) The medium of claim 14, wherein the second conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the first conditional access server.

16. (Original) The medium of claim 15, wherein the first conditional access server provides authorization to the second conditional access server according to an identity of the second conditional access server; the second conditional access server provides authorization to the client according to an identity of the client; and the first conditional access server is not aware of an identity of the client.

17. (Original) The medium of claim 10, wherein the second set of cryptographic keys consists one key.

18. (Original) The medium of claim 10, wherein the second conditional access server is a server of a further secondary conditional access server and acts as a primary conditional access server with respect to the further secondary conditional access server.

19. (Currently Amended) A secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

IPR2025-00305
ASUS EX1002 Page 560

a communication interface, the communication interface to receive a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys in a first security domain; and

a controller coupled to the communication interface, the controller to authorize a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server;

wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain, and

wherein the primary conditional access server authenticates the second conditional access server as one of clients of the primary conditional access server through a first authentication process using a first root of trust and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitue the first security domain with the second security domain for the client devices under the second root of trust.

IPR2025-00305
ASUS EX1002 Page 561

20. (Original) The secondary conditional access server of claim 19, wherein the controller is to translate authorization to access the content from authorization received from the primary conditional access server to authorization for the client.

21. (Original) The secondary conditional access server of claim 20, wherein the second set of cryptographic keys comprises a key of a digital rights management system; the client comprises a digital rights management client; and the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server.

22. (Original) The secondary conditional access server of claim 20, wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of the client; and the primary conditional access server is not aware of an identity of the client.

23. (Currently Amended) A secondary conditional access server to control a presentation of content, the secondary conditional access server comprising:

means for receiving a first set of cryptographic keys from a primary conditional access server which provides a representation of content in an encrypted form and authorizes access to the content through the first set of cryptographic keys in a first security domain; and

means for authorizing a client of the secondary conditional access server to present the content in accordance with authorization the secondary conditional access server received from the primary conditional access server;

wherein the secondary conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain, and

wherein the primary conditional access server authenticates the second conditional access server as one of clients of the primary conditional access server through a first authentication process using a first root of trust and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.

24. (Previously Presented) The secondary conditional access server of claim 23, further comprising:

means for recording a representation of the content in an encrypted form in response to a message from the primary conditional access server,

wherein the client sends a request, through a network connection to the secondary conditional access server, for authorization to present the content after the primary

conditional access server provides at least a portion of the content which is recorded; and

the secondary conditional access server obtains authorization from the primary conditional access server, after the primary conditional access server provides the portion of the content, for authorizing the client to present the content.

25. (Previously Presented) The secondary conditional access server of claim 23, further comprising:

means for translating authorization to access the content from authorization received from the primary conditional access server to authorization for the client,

wherein the second set of cryptographic keys comprises a key of a digital rights management system; and

the client comprises a digital rights management client; and

wherein the secondary conditional access server authorizes the client to use the content through the digital rights management system in accordance with authorization received from the primary conditional access server.

26. (Original) The secondary conditional access server of claim 23, wherein the primary conditional access server provides authorization to the secondary conditional access server according to an identity of the secondary conditional access server; the secondary conditional access server provides authorization to the client according to an identity of the client; and the primary conditional access server is not aware of an identity of the client.

27. (Original) The secondary conditional access server of claim 23, wherein the second set of cryptographic keys consists one key.

28. (Currently Amended) A method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component;

broadcasting the media component from a first conditional access server in a first security domain;

receiving a client request to use the media component from a client of a second conditional access server in a second security domain after said broadcasting; and

responding to the client request from the client of the second conditional access server,

wherein the first conditional access server authenticates the second conditional access server as one of clients of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

29. (Original) The method of claim 28, further comprising:

broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

30. (Original) The method of claim 29, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

31. (Original) The method of claim 30, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

32. (Currently Amended) A method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system in a first security domain;

processing the security messages on the conditional access server; and

transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

IPR2025-00305
ASUS EX1002 Page 566

wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

33. (Original) The method of claim 32, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system.

34. (Original) The method of claim 32, wherein the access controlled data is protected using a digital rights management system.

35. (Original) The method of claim 34, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

36. (Original) The method of claim 34, further comprising:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

37. (Original) The method of claim 36, wherein the access controlled data comprises a decrypted version of the entitlement control message.

38. (Original) The method of claim 34, further comprising:

receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

39. (Original) The method of claim 38, further comprising:

storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

40. (Original) The method of claim 32, further comprising:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

41. (Original) The method of claim 40, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

42. (Original) The method of claim 41, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

43. (Original) The method of claim 41, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

44. (Original) The method of claim 41, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

45. (Original) The method of claim 44, wherein the access controlled data further comprises the first and second control words.

46. (Original) The method of claim 32, further comprising:

receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

generating a second entitlement control message containing a second control word that is different from the first control word; and

descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

47. (Original) The method of claim 46, further comprising:

storing, at the conditional access server, the content rescrambled by the second control word; and

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

48. (Currently Amended) A method to process media content provided by a primary security system, the method comprising:

receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access

controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain,

wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

49. (Original) The method of claim 48, wherein the security message is an entitlement message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

50. (Original) The method of claim 48, wherein the access controlled format protects access to data using a digital rights management system.

51. (Original) The method of claim 50, further comprising:

automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

descrambling and recording the portion of the media content in response to a determination to descramble; and

recording the portion of the media content without descrambling in response to a determination not to descramble.

52. (Original) The method of claim 50, further comprising:

sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

53. (Original) The method of claim 52, further comprising:

descrambling media content using the control word; and

storing the media content in a storage under protection of a digital rights management system.

54. (Original) The method of claim 52, further comprising:

descrambling media content using the control word; and

rendering the media content for presentation.

55. (Original) The method of claim 54, further comprising:

retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

56. (Original) The method of claim 52, wherein the access controlled data comprises a decrypted version of the entitlement control message.

57. (Original) The method of claim 50, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

58. (Original) The method of claim 48, further comprising:

receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

59. (Original) The method of claim 58, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the method further comprises:

storing the second entitlement control message with the portion of the media content.

60. (Original) The method of claim 59, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

61. (Original) The method of claim 59, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further comprises:

descrambling the content using the first control word and rescrambling the content using the second control word.

62. (Currently Amended) A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to provide conditional access, the method comprising:

broadcasting a first entitlement management message for a subscriber to request caching of a media component;

broadcasting the media component from a first conditional access server in a first security domain;

IPR2025-00305
ASUS EX1002 Page 574

receiving a client request to use the media component from a client of a second conditional access server in a second security domain after said broadcasting; and

responding to the client request from the client of the second conditional access server,

wherein the first conditional access server authenticates the second conditional access server as one of clients of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates clients of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

63. (Original) The medium of claim 62, wherein the method further comprises:

broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

64. (Original) The medium of claim 63, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

65. (Original) The medium of claim 64, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

66. (Currently Amended) A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process conditional access protection, the method comprising:

receiving, at a conditional access server, security messages of a primary security system in a first security domain;

processing the security messages on the conditional access server; and

transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is

configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

67. (Original) The medium of claim 66, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said processing the entitlement management messages comprises:

decrypting to obtain a service key of the primary security system.

68. (Original) The medium of claim 66, wherein the access controlled data is protected using a digital rights management system.

69. (Original) The medium of claim 68, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

70. (Original) The medium of claim 68, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

71. (Original) The medium of claim 70, wherein the access controlled data comprises a decrypted version of the entitlement control message.

72. (Original) The medium of claim 68, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

73. (Original) The medium of claim 72, wherein the method further comprises:

storing, at the conditional access server, the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

74. (Original) The medium of claim 66, wherein the method further comprises:

receiving, at the conditional access server, an entitlement control message of the primary security system; and

processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

75. (Original) The medium of claim 74, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

76. (Original) The medium of claim 75, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

77. (Original) The medium of claim 75, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

78. (Original) The medium of claim 75, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

79. (Original) The medium of claim 78, wherein the access controlled data further comprises the first and second control words.

80. (Original) The medium of claim 66, wherein the method further comprises:

receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

generating a second entitlement control message containing a second control word that is different from the first control word; and

descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

81. (Original) The medium of claim 80, wherein the method further comprises:

storing, at the conditional access server, the content rescrambled by the second control word; and

retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

82. (Currently Amended) A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to process media content provided by a primary security system, the method comprising:

receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain,

wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of

the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured substitute the first security domain with the second security domain for the clients under the second root of trust.

83. (Original) The medium of claim 82, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

84. (Original) The medium of claim 82, wherein the access controlled format protects access to data using a digital rights management system.

85. (Original) The medium of claim 84, wherein the method further comprises:

automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

descrambling and recording the portion of the media content in response to a determination to descramble; and

recording the portion of the media content without descrambling in response to a determination not to descramble.

86. (Original) The medium of claim 84, wherein the method further comprises:

sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

87. (Original) The medium of claim 86, wherein the method further comprises:

descrambling media content using the control word; and

storing the media content in a storage under protection of a digital rights management system.

88. (Original) The medium of claim 86, wherein the method further comprises:

descrambling media content using the control word; and

rendering the media content for presentation.

89. (Original) The medium of claim 88, wherein the method further comprises:

retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

90. (Original) The medium of claim 86, wherein the access controlled data comprises a decrypted version of the entitlement control message.

91. (Original) The medium of claim 84, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

92. (Original) The medium of claim 82, wherein the method further comprises:

receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

93. (Original) The medium of claim 92, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the method further comprises:

storing the second entitlement control message with the portion of the media content.

94. (Original) The medium of claim 93, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

95. (Original) The medium of claim 93, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the method further comprises:

descrambling the content using the first control word and rescrambling the content using the second control word.

96. (Currently Amended) A primary security system to provide conditional access, the system comprising:

means for broadcasting a first entitlement management message for a subscriber to request caching of a media component;

means for broadcasting the media component, the primary security system being in a first security domain;

means for receiving a client request to use the media component from a client of a secondary conditional access server in a second security domain after said broadcasting; and

means for responding to the client request from the client of the secondary conditional access server,

wherein the primary security system authenticates the secondary conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first

IPR2025-00305
ASUS EX1002 Page 584

authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

97. (Original) The system of claim 96, further comprising:

means for broadcasting a second entitlement management message to authorize the client to playback the media component responsive to the client request.

98. (Original) The system of claim 97, wherein the client is not authorized to use the portion of the media content before the second entitlement management message.

99. (Original) The system of claim 98, wherein the second entitlement management message contains data specifying rights of the client to use the portion of the media content on a plurality of devices that are capable of using the portion of the media content simultaneously.

100. (Currently Amended) A data processing system to process conditional access protection, the data processing system comprising:

means for receiving, at a conditional access server, security messages of a primary security system in a first security domain;

means for processing the security messages on the conditional access server; and

means for transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured substitute the first security domain with the second security domain for the clients under the second root of trust.

101. (Previously Presented) The data processing system of claim 100, wherein the security messages comprise entitlement management messages; the conditional access server has a user key representing a subscriber of the primary security system; and said means for processing the entitlement management messages comprises:

means for decrypting to obtain a service key of the primary security system.

102. (Original)The data processing system of claim 100, wherein the access controlled data is protected using a digital rights management system.

103. (Original)The data processing system of claim 102, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

104. (Original)The data processing system of claim 102, further comprising:

means for receiving, at the conditional access server, an entitlement control message of the primary security system; and

means for processing the entitlement control message on the conditional access server to obtain a control word of the primary security system;

wherein the access controlled data comprises the control word.

105. (Original)The data processing system of claim 104, wherein the access controlled data comprises a decrypted version of the entitlement control message.

106. (Original)The data processing system of claim 102, further comprising:

means for receiving, at the conditional access server, an entitlement control message and scrambled content of the primary security system; and

means for descrambling the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

107. (Original)The data processing system of claim 106, further comprising:

means for storing, at the conditional access server, the content in an encrypted form;

IPR2025-00305
ASUS EX1002 Page 587

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

108. (Original)The data processing system of claim 100, further comprising:

means for receiving, at the conditional access server, an entitlement control message of the primary security system; and

means for processing the entitlement control message on the conditional access server to generate a substitutive entitlement control message as a replacement of the entitlement control message;

wherein the access controlled data comprises the substitutive entitlement control message.

109. (Original)The data processing system of claim 108, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

110. (Original)The data processing system of claim 109, wherein the substitutive entitlement control message is to be decrypted using a user key of the conditional access server for the primary security system.

111. (Original)The data processing system of claim 109, wherein the entitlement control message and the substitutive entitlement control message have a same control word.

112. (Original)The data processing system of claim 109, wherein the entitlement control message has a first control word; the substitutive entitlement control message has a second control word; and the first and second control words are different.

113. (Original)The data processing system of claim 112, wherein the access controlled data further comprises the first and second control words.

114. (Original)The data processing system of claim 100, further comprising:

means for receiving, at the conditional access server, a first entitlement control message containing a first control word and content scrambled by the first control word;

means for generating a second entitlement control message containing a second control word that is different from the first control word; and

means for descrambling the content using the first control word and rescrambling the content by the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

115. (Original)The data processing system of claim 114, further comprising:

means for storing, at the conditional access server, the content rescrambled by the second control word; and

means for retrieving the content rescrambled by the second control word in response to a request from the secondary conditional access client.

116. (Currently Amended) A data processing system to process media content provided by a primary security system, the data processing system comprising:

means for receiving, at a secondary conditional access client from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of the primary security system in a first security domain, the secondary conditional access client being in a second security domain,

wherein the primary security system authenticates the conditional access server clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

117. (Original)The data processing system of claim 116, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

118. (Original)The data processing system of claim 116, wherein the access controlled format protects access to data using a digital rights management system.

119. (Original)The data processing system of claim 118, further comprising:

means for automatically determining whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data;

means for descrambling and recording the portion of the media content in response to a determination to descramble; and

means for recording the portion of the media content without descrambling in response to a determination not to descramble.

120. (Original)The data processing system of claim 118, further comprising:

means for sending, from the secondary conditional access client to the conditional access server through a network connection, an entitlement control message, the entitlement control message containing a control word in an encrypted form;

wherein the access controlled data comprises the control word.

121. (Original)The data processing system of claim 120, further comprising:

means for descrambling media content using the control word; and

means for storing the media content in a storage under protection of a digital rights management system.

IPR2025-00305
ASUS EX1002 Page 591

122. (Original)The data processing system of claim 120, further comprising:

means for descrambling media content using the control word; and

means for rendering the media content for presentation.

123. (Original)The data processing system of claim 122, further comprising:

means for retrieving the entitlement control message from a storage device;

wherein the entitlement control message is controlled by a first entitlement management message for a first time period, which is earlier than a second entitlement management message for a second time period including a time between when the entitlement control message is sent from the secondary conditional access client to the conditional server and when the access controlled data is received at the secondary conditional access client.

124. (Original)The data processing system of claim 120, wherein the access controlled data comprises a decrypted version of the entitlement control message.

125. (Original)The data processing system of claim 118, wherein the access controlled data comprises a result of descrambling media content scrambled by a conditional access system of the primary security system.

126. (Original)The data processing system of claim 116, further comprising:

means for receiving a first entitlement control message for descrambling a portion of media content received from the primary security system; and

means for sending the first entitlement control message from the secondary conditional access client to the conditional access server through a network connection.

127. (Original)The data processing system of claim 126, wherein the access controlled data comprises a second entitlement control message as a replacement of the entitlement control message; and the system further comprises:

means for storing the second entitlement control message with the portion of the media content.

128. (Original)The data processing system of claim 127, wherein both the first and the second entitlement control messages contain a same control word; the second entitlement control message is encrypted to be decrypted using a key of the conditional access server.

129. (Original)The data processing system of claim 127, wherein the first entitlement control message contains a first control word; the second entitlement control message contains a second control word; the first and second control words are different; the access controlled data further comprises the first and second control words; and the system further comprises:

means for descrambling the content using the first control word and rescrambling the content using the second control word.

130. (Currently Amended) A conditional access server, comprising:

one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system in a first security domain;

a processor coupled to the one or more communication interfaces, the processor to process the security messages, and the one or more communication interfaces to transmit, to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,

wherein the primary security system authenticates the conditional access server clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

131. (Original)The conditional access server of claim 130, wherein the security messages comprise entitlement management messages; and the access controlled data is protected using a digital rights management system.

132. (Original)The conditional access server of claim 131, wherein rights to the access controlled data are at least partially derived from the entitlement management messages.

133. (Original)The conditional access server of claim 131, wherein the one or more communication interfaces are to receive an entitlement control message of the primary security system; the processor is to obtain a control word of the primary security system from the entitlement control message; and the access controlled data comprises the control word.

134. (Original)The conditional access server of claim 131, wherein the one or more communication interfaces are to receive an entitlement control message and scrambled content of the primary security system; and the conditional access server further comprises:

a descrambler coupled to the processor, the descrambler to descramble the scrambled content according to the entitlement control message;

wherein the access controlled data comprises a result of descrambling the scrambled content.

135. (Original)The conditional access server of claim 134, further comprising:

a storage device coupled to one or more communication interfaces, the storage device to store the content in an encrypted form;

wherein the access controlled data is provided in response to a request from the secondary conditional access client.

136. (Previously Presented) The conditional access server of claim 130, wherein the one or more communication interfaces are to receive entitlement control message of the primary security system; the processor is to generate a substitutive entitlement control message as a replacement of the entitlement control message; and the access controlled data comprises the substitutive entitlement control message.

137. (Original)The conditional access server of claim 136, wherein the substitutive entitlement control message has a control word encrypted using a key of the conditional access server.

138. (Original)The conditional access server of claim 130, wherein the one or more communication interfaces are to receive a first entitlement control message containing a first control word and content scrambled by the first control word; the processor is to generate a second entitlement control message containing a second control word that is different from the first control word; and the conditional access server further comprises:

a transcrambler coupled to the one or more communication interfaces and the processor, the transcrambler to descramble the content using the first control word and rescramble the content using the second control word;

wherein the access controlled data comprises the content rescrambled by the second control word and second entitlement control message.

139. (Original)The conditional access server of claim 138, further comprising:

a storage device coupled to the transcrambler, the storage device to store the content rescrambled by the second control word.

140. (Currently Amended) A secondary conditional access client, comprising:

a communication interface to receive, from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system in a first security domain, the secondary conditional access client being in a second security domain; and

a processor coupled to the communication interface, the processor to process the access controlled data,

wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

IPR2025-00305
ASUS EX1002 Page 597

141. (Original)The client of claim 140, wherein the security message is an entitlement management message; and wherein the secondary conditional access client does not have a user key representing a subscriber of the primary security system.

142. (Original)The client of claim 140, wherein the access controlled format protects access to data using a digital rights management system.

143. (Original)The client of claim 142, wherein the processor is to automatically determine whether or not to descramble a portion of media content received from the primary security system for recording according to the entitlement data; the client further comprises:

a storage device;

a descrambler coupled to the processor and the storage device, in response to a determination to descramble the descrambler to descramble the portion of the media content for storing in the storage device, in response to a determination not to descramble the storage device to record the portion of the media content without descrambling.

144. (Original)The client of claim 142, wherein the communication interface is to send, to the conditional access server through a network connection, an entitlement control message containing a control word in an encrypted form; and the access controlled data comprises the control word.

145. (Original)The client of claim 144, further comprising:

a storage device;

a descrambler coupled to the processor and the storage device, the descrambler to descramble media content using the control word, the storage device to store the media content under protection of a digital rights management system.

146. (Previously Presented) The client of claim 140, further comprising:

a physical interface to receive a first entitlement control message for descrambling a portion of media content received from the primary security system; and

wherein the communication interface is to send the first entitlement control message to the conditional access server through a network connection.

EX1002 - Page 599

IPR2025-00305
ASUS EX1002 Page 599

REMARKS

Reconsideration of this application, as amended, is respectfully requested.

Claims 1-146, are pending. Claims 1-146 stand rejected.

Claims 1, 10, 19, 23, 28, 32, 48, 62, 66, 82, 96, 100, 116, 130, and 140 have been amended. No claims have been canceled. No claims have been added. Support for the amendments is found in the specification, the drawings, and in the claims as originally filed. Applicant submits that the amendments do not add new matter.

Applicant reserves all rights with respect to the applicability of the Doctrine of Equivalents.

Claims 10-18 and 62-95 were rejected under 35 U.S.C § 101.

Applicant has amended independent claims 10, 62, 66, and 82 to include "non-transitory".

Therefore, applicant respectfully submits that the Examiner's rejections of claims 10, 62, 66, and 82 under 35 U.S.C § 101 have been overcome.

Given that dependent claims 11-18, 63-65, 67-81, and 83-95 depend from amended independent claims 0, 62, 66, and 82 respectively, and add additional limitations, applicant respectfully submits that the Examiner's rejection of dependent claims 11-18, 63-65, 67-81, and 83-95 under 35 U.S.C. § 101 have been overcome.

Claims 1-35, 37-40, 48-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132, 134-136, 137, 140-143 and 146 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent No. 7,036,011 to Grimes (hereinafter "Grimes") and further in view of U.S. Patent No. 7,493,291 to Simelius (hereinafter "Simelius"), and further in view of U.S. Patent No. 6,961,858 to Fransdonk (hereinafter "Fransdonk").

Amended claim 1 reads, as follows:

A method to control a presentation of content, the method comprising:
receiving a representation of content from a first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access in a first security domain; and
presenting the content, at a user's request, through a second conditional access server which is coupled to the first conditional access server;
wherein the presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively;
wherein the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain; and
wherein the first conditional access server authenticates the second conditional access server as one of client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.

(emphasis added).

The Examiner acknowledged that Grimes fails to teach "wherein the first conditional access server authenticates client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process." (Office Action, page 5). The Examiner acknowledged that Simelius and Grimes do not disclose "wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust." (Office Action, page 6). The Examiner suggests that Fransdonk's "logically separating user authentication functionality from content security" and "verification of

IPR2025-00305
ASUS EX1002 Page 601

two separate certificates, namely a first user device certificate for user authentication and a second secure copy-protected device certificate for content security authentication" teaches the above limitations. Applicant respectfully disagrees.

Grimes discloses that "only those clients that purchased the PPV content or the subscription, or that meet the restriction, will receive the digital certificate (col. 7, lines 15-18). Thus, Grimes discloses receiving the server digital certificate by the clients. In contrast, amended claim 1 refers to a second conditional access server as one of the clients of the first conditional access server. Grimes is silent about a second conditional access server acting as one of the clients of the first conditional access server.

Accordingly, Grimes fails to teach or suggest a first conditional access server that authenticates a second conditional access server as one of client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, as recited in amended claim 1.

Furthermore, Grimes fails to teach or suggest that the first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access in a first security domain and that the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain, and wherein the second conditional access server is configured to substitute the first security domain with the

second security domain for the client devices under the second root of trust, as recited in amended claim 1.

Simelius, in contrast, discloses a system that has a content provider server, and a plurality of clients that receive the content from the content provider server (Figure 1). More specifically, Simelius discloses that the content provider server 102 sends the voucher 114 comprising child vouchers 114', to parent client 106, which in turn forwards the child vouchers 114' to the respective child clients, such as child client 116, and the content provider server 102 sends the voucher 138 comprising child vouchers 138', to parent client 134, which in turn forwards the child vouchers 138' to the respective child clients, such as child client 140 (Figure 1). In particular, Simelius discloses that the child vouchers are verified against the right of use vouchers (col. 13, lines 38-50).

Thus, Simelius discloses verifying the child clients. In contrast, amended claim 1 refers to a first conditional access server authenticating a second conditional access server as one of client devices of the first conditional access server. Simelius fails to teach or suggest a first conditional access server authenticating a second conditional access server as one of client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticating client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, as recited in amended claim 1.

Furthermore, Simelius fails to teach or suggest the first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access in a first security domain and the second conditional access

server which uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain, and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust, as recited in amended claim 1.

Fransdonk, in contrast, discloses content distribution system which deploys distributed conditional access agents 28 to represent interests of the content providers 16 (Figures 1 and 16). More specifically, Fransdonk discloses that security functionality is implemented by agents 28 (col. 22, lines 17-27). Figure 16 of Fransdonk shows that conditional access agent 28 is connected through conditional access client 48 to secure user authentication device 402 and secure copy protected device 408. In particular, Fransdonk discloses that the agent 28 verifies via the client 48 two separate certificates, such as a user device certificate for user authentication and a secure copy-protected device certificate for content security authentication (col. 34, lines 33-50).

Thus, Fransdonk discloses verifying, in parallel, two identities of the same client device. In contrast, amended claim 1 refers to the first conditional access server authenticating the second conditional access server.

Fransdonk fails to teach or suggest a first conditional access server authenticating a second conditional access server as one of client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticating client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, as recited in amended claim 1.

Furthermore, Fransdonk discloses two authentication processes that run in parallel for the same client device, while amended claim 1 reciting the first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access in a first security domain and the second conditional access server which uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain, wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust refers to the two authentication processes that run in serial. Therefore, Fransdonk teaches away from amended claim 1.

As set forth above, Grimes, Simelius, and Fransdonk address technologies that are totally different from those addressed by amended claim 1. One of ordinary skill in the art would not use Grimes, Simelius, and Fransdonk to arrive at the limitations, as claimed in amended claim 1.

Furthermore, even if Grimes, Simelius, and Fransdonk were combined, such a combination would still lack a first conditional access server authenticating a second conditional access server as one of client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticating client devices of the second conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, as recited in amended claim 1.

Moreover, even if Grimes, Simelius, and Fransdonk were combined, such a combination would still lack the first conditional access server which provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access in

EX1002 - Page 605
IPR2025-00305
ASUS EX1002 Page 605

a first security domain and the second conditional access server which uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain, wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust, as recited in amended claim 1.

Therefore, applicant respectfully submits that claim 1, as amended, is not obvious over Grimes, and further in view of Simelius, and further in view of Fransdonk under 35 U.S.C. §103(a).

Given that claims 2-35, 37-40, 48-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132, 134-136, 137, 140-143 and 146 contains some limitations that are similar to those limitations set forth above, applicant respectfully submits that claims 2-35, 37-40, 48-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132, 134-136, 137, 140-143 and 146 are not obvious under 35 U.S.C. §103(a) over Grimes, and further in view of Simelius, and further in view of Fransdonk.

Claims 36, 41-47, 52-56, 60, 61, 70, 75-81, 86-90, 94, 95, 104, 109-115, 120-124, 128, 129, 133, 137-139, 144 and 145 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Grimes, Simelius, and Fransdonk as applied to claims 32, 66, 100, 130 and 140 above, and further in view of U. S. Patent No. 7,302,058 to Candelore (hereinafter "Candelore").

In view of the above discussion, it is respectfully submitted that even if Grimes, Simelius, and Fransdonk were combined, such a combination would still lack receiving, at a conditional access server, security messages of a primary security system in a first security domain; processing the security messages on the conditional access server; and transmitting, from the conditional access server to a secondary conditional access client through a network connection

in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages, wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust, as recited in amended claim 32.

Candelore, in contrast, discloses securing control words. Candelore fails to teach or suggest receiving, at a conditional access server, security messages of a primary security system in a first security domain; processing the security messages on the conditional access server; and transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages, wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured to substitute

EX1002 - Page 607
IPR2025-00305
ASUS EX1002 Page 607

the first security domain with the second security domain for the clients under the second root of trust, as recited in amended claim 32.

As set forth above, Candelore, Grimes, Simelius, and Fransdonk address technologies that are totally different from those addressed by amended claim 1. One of ordinary skill in the art would not use Candelore, Grimes, Simelius, and Fransdonk to arrive at the limitations, as claimed in amended claim 1.

Furthermore, even if Grimes, Simelius, and Fransdonk were combined, such a combination would still lack receiving, at a conditional access server, security messages of a primary security system in a first security domain; processing the security messages on the conditional access server; and transmitting, from the conditional access server to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages, wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, and wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust, as recited in amended claim 32.

Given that claims 36, 41-47, 52-56, 60, 61, 70, 75-81, 86-90, 94, 95, 104, 109-115, 120-124, 128, 129, 133, 137-139, 144 and 145 contain some limitations that are similar to those limitations set forth above, applicant respectfully submits that claims 36, 41-47, 52-56, 60, 61,

70, 75-81, 86-90, 94, 95, 104, 109-115, 120-124, 128, 129, 133, 137-139, 144 and 145 are not obvious under 35 U.S.C. §103(a) over Grimes, Simelius, and Fransdonk, and further in view Candelore.

EX1002 - Page 609
IPR2025-00305
ASUS EX1002 Page 609

It is respectfully submitted that in view of the amendments and arguments set forth herein, the applicable rejections and objections have been overcome. If the Examiner believes a telephone conference would expedite the prosecution of the present application, the Examiner is invited to call the undersigned at (408) 720-8300.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: May 1, 2012

/Tatiana Rossin/
Tatiana Rossin
Reg. No. 56,833

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

Customer No. 08791

Electronic Patent Application Fee Transmittal

Application Number:	11007116
Filing Date:	07-Dec-2004
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Filer:	Tatiana Rossin/Betty Scaletta
Attorney Docket Number:	6517P002

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	150	150

IPR2025-00305
ASUS EX1002 Page 611

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**150**

IPR2025-00305
ASUS EX1002 Page 612

Electronic Acknowledgement Receipt	
EFS ID:	12680173
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	Tatiana Rossin/Betty Scaletta
Filer Authorized By:	Tatiana Rossin
Attorney Docket Number:	6517P002
Receipt Date:	01-MAY-2012
Filing Date:	07-DEC-2004
Time Stamp:	20:54:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$150
RAM confirmation Number	7809
Deposit Account	022666
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

IPR2025-00305
ASUS EX1002 Page 613

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees) Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees) Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	6517P002_EOT_05-01-12.pdf	15863 d9df64a716ff2dd5746d3b69812eada1d4f92255	no	1
Warnings:					
Information:					
2		6517P002_R-OA_05-01-12.pdf	176342 1008846c95232d02790271de7dd6186a7a172b2d	yes	56

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	45
Applicant Arguments/Remarks Made in an Amendment	46	56

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	29752 3ac1dad12cb7d17a135a3581c1c045ca94f3548c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	221957		

IPR2025-00305
ASUS EX1002 Page 614

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Attorney's Docket No.: 6517P002 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor:	Examiner: Avery, Jeremiah L.
Luc Vantalon	Art Unit: 2431
Application No.: 11/007,116	Confirmation No.: 9254
Filed: December 7, 2004	**CERTIFICATE OF ELECTRONIC FILING** I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on: 05-01-2012 /Betty Scaletta/ Date Betty Scaletta
For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR EXTENSION OF TIME PURSUANT TO 37 C.F.R. § 1.136 (a)

Sir:

Applicant respectfully petitions pursuant to 37 CFR 1.136(a) for a one month extension of time to file this response to the Office Action mailed January 3, 2012. The extended period is set to expire on May 3, 2012. The Director is authorized to charge our Deposit Account No. 02-2666 in the amount of $150.00 for the fee under 37 C.F.R. § 1.17 (a)(1) for a one month extension of time.

Please charge any shortages and credit any overages to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: May 1, 2012

/Tatiana Rossin/
Tatiana Rossin
Reg. No. 56,833

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

IPR2025-00305
ASUS EX1002 Page 616

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/007,116	12/07/2004	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	05/01/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 146	Minus	** 146	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	* 15	Minus	***15	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/GLORIA ANTHONY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Attorney Docket No.: 6517P002 Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Luc Vantalon Application No. 11/007,116 Filed: December 7, 2004 For: Methods and apparatuses for secondary conditional access server	Examiner: Avery, Jeremiah L. Art Unit: 2431 Confirmation No. 9254 **CERTIFICATE OF TRANSMISSION** I hereby certify that this correspondence is being submitted electronically via EFS-Web on the date shown below. /Betty Scaletta/ 05-21-2012 ***Betty Scaletta*** ***Date***

E-filed via EFS-Web
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INTERVIEW CONFIRMATION AND PROPOSED AGENDA

Sir:

Following the teleconference between Tatiana Rossin and Examiner on May 17, 2012, this is to confirm that the interview is scheduled on May 29, 2012 at 1:00PM EST. It is proposed to discuss the amendment filed by applicant on May 1, 2012 in response to the Office Action mailed January 3, 2012, and receive the Examiner's feedback. Tentative participants are James C. Scheller and Tatiana Rossin. Tatiana Rossin will take responsibility for initiating the call on May 29, 2012, and will dial 1-571-272-8627 unless the Examiner recommends differently.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: May 21, 2012

/Tatiana Rossin/
Tatiana Rossin
Reg. No. 56,833

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300
Fax (408) 720-8383

IPR2025-00305
ASUS EX1002 Page 618

PTOL-413A (04-09)
Approved for use through 05/31/2009. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 11/007,116 First Named Applicant: Luc Vantalon

Examiner: Jeremiah L. Avery Art Unit: 2431 Status of Application: Pending

Tentative Participants:

(1) James C. Scheller (2) Tatiana Rossin

(3) _____ (4) _____

Proposed Date of Interview: May 29, 2012 **Proposed Time:** 1:00PM EST **AM/PM**

Type of Interview Requested:

(1) ☑ **Telephonic** (2) ☐ **Personal** (3) ☐ **Video Conference**

Exhibit To Be Shown or Demonstrated: ☐ **YES** ☐ **NO**

If yes, provide brief description: _____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Claim Rejections	1-35, 37-40, 48-51, 57-59, 62-69, 71-74, 82-85, 91-93, 96-103, 105-108, 114, 116-120, 125-127, 128, 130-132,	U. S. Patent No. 7,036,011; U.S. Patent No. 7,493,291; U.S. Patent No. 6,961,858	☐	☐	☐
(2)	36, 41-47, 52-56, 60, 61, 70, 75-81, 86-90, 94, 95, 104, 109-115, 120-124, 128, 129, 133, 137-139, 144	U. S. Patent No. 7,036,011; U.S. Patent No. 7,493,291; U.S. Patent No. 6,961,858; U. S. Patent No. 7,302,058	☐	☐	☐
(3)			☐	☐	☐
(4)			☐	☐	☐

☐ Continuation Sheet Attached

Brief Description of Argument to be Presented:

It is proposed to discuss the amendment filed by applicant on May 1, 2012 in response to the Office Action mailed January 3, 2012, and receive the Examiner's feedback.

An interview was conducted on the above-identified application on _____ **.**

NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).

This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

/Tatiana Rossin/
Applicant/Applicant's Representative Signature

Tatiana Rossin
Typed/Printed Name of Applicant or Representative

56,833
Registration Number, if applicable

Examiner/SPE Signature

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	12825409
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	Methods and apparatuses for secondary conditional access server
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	Tatiana Rossin/Betty Scaletta
Filer Authorized By:	Tatiana Rossin
Attorney Docket Number:	6517P002
Receipt Date:	21-MAY-2012
Filing Date:	07-DEC-2004
Time Stamp:	15:25:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Letter Requesting Interview with Examiner	6517P002_ExIntReq_052112.pdf	17629 6eee8aa6edf53301ccce037e0e7e610fd7d1a0c1	no	1

Warnings:	
Information:	

IPR2025-00305
ASUS EX1002 Page 620

2	Letter Requesting Interview with Examiner	6517P002_IntReqForm_052112.pdf	148104 14e557d8e849672f399c0aef4d451d4cf6a589fc	no	1

Warnings:	
Information:	
Total Files Size (in bytes):	165733

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IPR2025-00305
ASUS EX1002 Page 621

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

8791 7590 06/07/2012

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
06/07/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of Allowability	Application No.	Applicant(s)	
	11/007,116	VANTALON ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the amendment filed on 05/01/12*.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1-146*.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Jeremiah Avery/
Examiner, Art Unit 2431

Examiner's Statement of Reasons for Allowance

1. Claims 1-146 are allowed over the prior art.

2. This action is in reply to the Applicant's correspondence on 05/01/12.

3. The following is an Examiner's statement of reasons for the indication of allowable claimed subject matter.

4. The 35 U.S.C. 101 rejection of claims 10-18 and 62-95 is hereby withdrawn due to the Applicant's amendments.

5. As per independent claims 1, 10, 19, 23, 28, 32, 48, 62, 66, 82, 96, 100, 116, 130 and 140, generally, the prior art of record, United States Patent No. 7,036,011 to Grimes, United States Patent No. 7,493,291 to Simelius and United States Patent No. 6,961,858 to Fransdonk fails to teach alone, or in combination, other than via hindsight, at the time of the invention, the features as discussed and remarked upon in the response of 05/01/12.

6. Nowhere in the prior art is found, collectively, the *italicized* claim elements (i.e., *"wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust"*), at the time of the invention; serving to patently distinguish the invention from said prior art:

7. Claims 1, 10 and 28: "wherein the first conditional access server authenticates the second conditional access server as one of client devices of the first conditional access server through a first authentication process using a first root of trust and the second conditional access server authenticates client devices of the second conditional

access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, *and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust*."

8. Claims 19, 23 and 62 : "wherein the primary conditional access server authenticates the second conditional access server as one of clients of the primary conditional access server through a first authentication process using a first root of trust and the secondary conditional access server authenticates clients of the secondary conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, *and wherein the second conditional access server is configured to substitute the first security domain with the second security domain for the client devices under the second root of trust*."

9. Claims 32, 48, 66, 82, 96, 100, 116, 130 and 140: "wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust, *and wherein the conditional*

access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust."

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

11. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

12. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431
/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/007,116	Applicant(s)/Patent Under Reexamination VANTALON ET AL.	
	Examiner JEREMIAH AVERY	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,325,140	01-2008	Carley, Jeffrey Alan	713/182
*	B	US-2005/0021539	01-2005	Short et al.	707/100
*	C	US-6,961,858	11-2005	Fransdonk, Robert W.	726/29
*	D	US-7,152,160	12-2006	Lantto et al.	713/168
*	E	US-7,685,206	03-2010	Mathew et al.	707/785
*	F	US-7,493,291	02-2009	Simelius, Kim	705/59
*	G	US-2004/0196842	10-2004	Dobbins, Kurt A.	370/389
*	H	US-7,296,154	11-2007	Evans et al.	713/169
*	I	US-7,336,784	02-2008	Zuili, Patrick	380/200
*	J	US-7,316,032	01-2008	Tayebi et al.	705/51
*	K	US-7,292,692	11-2007	Bonan et al.	380/212
*	L	US-7,177,429	02-2007	Moskowitz et al.	380/252
*	M	US-7,036,011	04-2006	Grimes et al.	713/156

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Kamperman, Frank. van Rijnsoever, Bart. Conditional Access System Interoperability Through Software Downloading. IEEE Transactions on Consumer Electronics. Vol. 47. Issue: 1. Relevant Pages: 47-54. Pub. Date: Feb. 2001. Found on The World Wide Web at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=920419
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/30/2012								
	1	=								
	2	=								
	3	=								
	4	=								
	5	=								
	6	=								
	7	=								
	8	=								
	9	=								
	10	=								
	11	=								
	12	=								
	13	=								
	14	=								
	15	=								
	16	=								
	17	=								
	18	=								
	19	=								
	20	=								
	21	=								
	22	=								
	23	=								
	24	=								
	25	=								
	26	=								
	27	=								
	28	=								
	29	=								
	30	=								
	31	=								
	32	=								
	33	=								
	34	=								
	35	=								
	36	=								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/30/2012								
	37	=								
	38	=								
	39	=								
	40	=								
	41	=								
	42	=								
	43	=								
	44	=								
	45	=								
	46	=								
	47	=								
	48	=								
	49	=								
	50	=								
	51	=								
	52	=								
	53	=								
	54	=								
	55	=								
	56	=								
	57	=								
	58	=								
	59	=								
	60	=								
	61	=								
	62	=								
	63	=								
	64	=								
	65	=								
	66	=								
	67	=								
	68	=								
	69	=								
	70	=								
	71	=								
	72	=								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/30/2012								
	73	=								
	74	=								
	75	=								
	76	=								
	77	=								
	78	=								
	79	=								
	80	=								
	81	=								
	82	=								
	83	=								
	84	=								
	85	=								
	86	=								
	87	=								
	88	=								
	89	=								
	90	=								
	91	=								
	92	=								
	93	=								
	94	=								
	95	=								
	96	=								
	97	=								
	98	=								
	99	=								
	100	=								
	101	=								
	102	=								
	103	=								
	104	=								
	105	=								
	106	=								
	107	=								
	108	=								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/30/2012								
	109	=								
	110	=								
	111	=								
	112	=								
	113	=								
	114	=								
	115	=								
	116	=								
	117	=								
	118	=								
	119	=								
	120	=								
	121	=								
	122	=								
	123	=								
	124	=								
	125	=								
	126	=								
	127	=								
	128	=								
	129	=								
	130	=								
	131	=								
	132	=								
	133	=								
	134	=								
	135	=								
	136	=								
	137	=								
	138	=								
	139	=								
	140	=								
	141	=								
	142	=								
	143	=								
	144	=								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	**Art Unit**
	JEREMIAH AVERY	2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/30/2012								
	145	=								
	146	=								

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	**Art Unit**
	JEREMIAH AVERY	2431

ORIGINAL		INTERNATIONAL CLASSIFICATION														
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED									
713	189	H	0	4	L	29 / 06 (2006.01.01)										

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
713	153				
726	2	3	27		
348	E5.004	E7.06			

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		20		39		58		77		96		115		134
	2		21		40		59		78		97		116		135
	3		22		41		60		79		98		117		136
	4		23		42		61		80		99		118		137
	5		24		43		62		81		100		119		138
	6		25		44		63		82		101		120		139
	7		26		45		64		83		102		121		140
	8		27		46		65		84		103		122		141
	9		28		47		66		85		104		123		142
	10		29		48		67		86		105		124		143
	11		30		49		68		87		106		125		144
	12		31		50		69		88		107		126		145
	13		32		51		70		89		108		127		146
	14		33		52		71		90		109		128		
	15		34		53		72		91		110		129		
	16		35		54		73		92		111		130		

/JEREMIAH AVERY/ Examiner.Art Unit 2431	05/31/12	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	146	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2431	06/04/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2A

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	**Art Unit**
	JEREMIAH AVERY	2431

☒ Claims renumbered in the same order as presented by applicant	☐ CPA	☐ T.D.	☐ R.1.47

	17		36		55		74		93		112		131		
	18		37		56		75		94		113		132		
	19		38		57		76		95		114		133		

/JEREMIAH AVERY/ Examiner.Art Unit 2431	05/31/12	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	146	
/NATHAN FLYNN/ Supervisory Patent Examiner.Art Unit 2431	06/04/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2A

U.S. Patent and Trademark Office

Part of Paper No. 20120530

IPR2025-00305
ASUS EX1002 Page 634

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11007116	VANTALON ET AL.
	Examiner	Art Unit
	JEREMIAH AVERY	2431

SEARCHED			
Class	Subclass	Date	Examiner
713	189	5/31/2012	JLA
726	2	5/31/2012	JLA

SEARCH NOTES		
Search Notes	Date	Examiner
Keywords in EAST Search	5/31/2012	JLA
Inventor Search	5/31/2012	JLA
Keyword Search within Class 713, subclasses 153 and 189, Class 726, subclasses 2, 3 and 27 and Class 348, subclasses E5.004 and E7.06	5/31/2012	JLA
Assignee Search	5/31/2012	JLA
IEEE Search	5/31/2012	JLA
Discussed Search Strategy with Primary Examiner Christian LaForgia	5/29/2012	JLA

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
none	((conditional and access and (replac$3 or swap$4 or substitu$3 or switch$) and domain) and server and ($2crypt$ or $2cipher$)).clm.	5/31/2012	JLA

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	30	conditional near access and (replac$3 or swap$4 or substitut$3) with domain	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:26
L2	30	L1 and (replac$3 or swap$4 or substitut$3 or switch$) with domain	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:26
L3	1258	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:26
L4	1217	L3 and ((first or primary) or (second$3 or other or next or another) with ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) with (authentic$ or verify$ or verification)))	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:26
L5	158	L4 and (access near server)	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:26
L6	109	L5 and (server same (($2crypt$ or $2cipher) near key))	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:26
L7	83	L6 and ($2authoris$ or $2authoriz$)	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:26
L8	64	L7 and (($2authoris$ or $2authoriz$) with access$)	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:26
L9	1	L8 and (replac$3 or swap$4 or substitut$3 or switch$) with domain	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:26
L10	1	L8 and ((replac$3 or swap$4 or substitut$3 or switch$) with domain) and server	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:28
L11	6	(VANTALON-LUC.in. or SICCARDO-PAOLO.in.) and (access$ and ($2crypt$ or $2cipher$) and server).clm.	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:40
L12	2	(DIGITAL-KEYSTONE-INC.as.) and (access$ and ($2crypt$ or $2cipher$) and server).clm.	US-PGPUB;	OR	ON	2012/05/31 16:40

			USPAT; EPO			
L13	75	(713/189.ccls. or 713/153.ccls. or 726/2.ccls. or 726/3.ccls. or 726/27.ccls. or 348/E5.004.ccls. or 348/E7.06.ccls.) and (((replac$3 or swap$4 or substitut$3 or switch$) with domain) same server)	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:46
L14	71	l13 and access$	US-PGPUB; USPAT; EPO	OR	ON	2012/05/31 16:46
S1	990	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT	OR	ON	2009/03/26 19:43
S2	873	S1 and server	US-PGPUB; USPAT	OR	ON	2009/03/26 19:48
S3	522	S2 and unauthori$	US-PGPUB; USPAT	OR	ON	2009/03/26 19:49
S4	447	S3 and (authoris$ or authoriz$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:49
S5	433	S4 and (ID or identit$ or identif$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:50
S6	420	S5 and ((first or primary) or (second$ or other) near server)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:50
S7	402	S6 and (broadcast$ or transmit$ or transmission or send$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:52
S8	395	S7 and ((broadcast$ or transmit$ or transmission or send$) same (media or audio or video or stream or content or data or information))	US-PGPUB; USPAT	OR	ON	2009/03/26 19:52
S9	317	S8 and (play$ or playback)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:53
S10	150	S9 and (subscribe$ or subscript$)	US-PGPUB; USPAT	OR	ON	2009/03/26 19:54
S11	39	S10 and $2scrambl$	US-PGPUB; USPAT	OR	ON	2009/03/26 19:54
S12	7	S11 and (control$5 near word)	US-PGPUB; USPAT	OR	ON	2009/03/26 20:00
S13	1058	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S14	932	S13 and server	US-	OR	ON	2009/11/21

			PGPUB; USPAT			12:01
S15	556	S14 and unauthori$	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S16	477	S15 and (authoris$ or authoriz$)	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S17	461	S16 and (ID or identit$ or identif$)	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S18	448	S17 and ((first or primary) or (second$ or other) near server)	US-PGPUB; USPAT	OR	ON	2009/11/21 12:01
S19	448	S18 and ((first or primary) or (second$ or other) near (authentic$ or verify$ or verification))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:02
S20	448	S19 and ((first or primary) or (second$ or other or next) near ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:06
S21	0	S20 and (((first or primary) or (second$ or other or next) near (access near server)) near ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:08
S22	7	S20 and (((first or primary) or (second$ or other or next) near (access near server)) same ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:09
S23	7	S20 and (((first or primary) or (second$ or other or next) near server) same ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:22
S24	0	S20 and (((first or primary) or (second$ or other or next) near server) near ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification)))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:23
S25	55	S20 and (((first or primary) or (second$ or other or next) near server) near (authentic$ or verify$ or verification))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:24
S26	11	S25 and ((different or unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) near (authentic$ or verify$ or verification))	US-PGPUB; USPAT	OR	ON	2009/11/21 12:25
S27	1236	control$5 and (($2crypt$ or $2cipher$) near key) and ($2crypt$ or $2cipher$) and access$ and (content or data or information) and (DRM or (Digital near rights near managment)) and (@ad<"20041207" @prad<"20041207")	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:08
S28	1195	S27 and ((first or primary) or (second$3 or other or next or another) with ((different or	US-PGPUB;	OR	ON	2011/12/20 16:12

		unique or variant or dissimilar or independent or autonomous or separate or unrelat$4) with (authentic$ or verify$ or verification)))	USPAT; EPO			
S29	158	S28 and (access near server)	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:13
S30	109	S29 and (server same (($2crypt$ or $2cipher) near key))	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:19
S31	83	S30 and ($2authoris$ or $2authoriz$)	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:24
S32	64	S31 and (($2authoris$ or $2authoriz$) with access$)	US-PGPUB; USPAT; EPO	OR	ON	2011/12/20 16:25
S33	30	conditional near access and (replac$3 or swap$4 or substitut$3) with domain	US-PGPUB; USPAT; EPO	OR	ON	2012/05/29 11:40

5/ 31/ 2012 4:51:58 PM
C:\ Users\ javery\ Documents\ EAST\ Workspaces\ 11007116.wsp

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L15	0	((conditional near access and (replac$3 or swap$4 or substitu$3 or switch$) with domain) and server and ($2crypt$ or $2cipher$)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2012/05/31 16:50
L16	6	((conditional and access and (replac$3 or swap$4 or substitu$3 or switch$) and domain) and server and ($2crypt$ or $2cipher$)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2012/05/31 16:51

5/ 31/ 2012 4:51:45 PM
C:\ Users\ javery\ Documents\ EAST\ Workspaces\ 11007116.wsp

SEARCH RESULTS

You searched for: ((conditional access) AND domain) AND authorization)

You Refined by:

Publisher: IEEE, AIP, IET, IBM

Content Type: Conference Publications, Journals & Magazines

Topic: Computing & Processing (Hardware/Software), Components, Circuits, Devices & Systems, Communication, Networking & Broadcasting, Signal Processing & Analysis

Publication Year: 1972 - 2004

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

8791 7590 06/08/2012

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER
AVERY, JEREMIAH L

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 06/08/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

TITLE OF INVENTION: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	09/10/2012

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 02/11)

IPR2025-00305
ASUS EX1002 Page 642

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

8791 7590 06/08/2012

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

TITLE OF INVENTION: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	09/10/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
AVERY, JEREMIAH L	2431	713-189000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

8791 7590 06/08/2012

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2431	

DATE MAILED: 06/08/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 1728 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 1728 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IPR2025-00305
ASUS EX1002 Page 645

Applicant-Initiated Interview Summary	**Application No.** 11/007,116	**Applicant(s)** VANTALON ET AL.	
	Examiner JEREMIAH AVERY	**Art Unit** 2431	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Jeremiah Avery*.

(2) *Tatiana Rossin*.

(3) *James C. Scheller*.

(4) *Luc Vantalon*.

Date of Interview: *29 May 2012*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *United States Patent No. 7,036,011 to Grimes et al., United States Patent No. 7,493,291 to Simelius and United States Patent No. 6,961,858 to Fransdonk*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

The filed amendments to the claims were discussed; in particular, the substitution of the security domains. The Examiner made note of the amendments to said claims as well as the Applicant's arguments regarding how these amendments help distinguish the claimed invention from the cited prior art. The Examiner will conduct an updated search, focusing on the amendments filed..

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Jeremiah Avery/ Examiner, Art Unit 2431	/NATHAN FLYNN/ Supervisory Patent Examiner, Art Unit 2431

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

———

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IPR2025-00305
ASUS EX1002 Page 647

Attorney's Docket No.: 6517P002 Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor: Luc Vantalon Application No. 11/007,116 Filed: December 7, 2004 For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	Examiner: Avery, Jeremiah L. Art Unit: 2431 Confirmation No.: 9254 **Certificate of E-Filing** I hereby certify that this correspondence is being electronically deposited with the USPTO via EFS-Web: On: 07-02-2012 By: /Betty Scaletta/ Betty Scaletta

Commissioner for Patents
Alexandria, VA 22313-1450

RESPONSE TO INTERVIEW SUMMARY

Sir:

Please enter the following response to the Interview Summary mailed June 8, 2012. Applicant agrees with the Examiner and the summary of the telephonic interview of May 29, 2012, regarding the proposed claim changes which were carried out by the Amendment filed by applicant on May 1, 2012.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: July 2, 2012

/Tatiana Rossin/
Tatiana Rossin
Reg. No. 56,833

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

IPR2025-00305
ASUS EX1002 Page 648

Electronic Acknowledgement Receipt	
EFS ID:	13165037
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	Tatiana Rossin/Betty Scaletta
Filer Authorized By:	Tatiana Rossin
Attorney Docket Number:	6517P002
Receipt Date:	02-JUL-2012
Filing Date:	07-DEC-2004
Time Stamp:	20:57:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant summary of interview with examiner	6517P002_R-IntSum_07-02-12.pdf	19857 01926c29a3c0d74d178bd09e997fa5458950fa86	no	1

Warnings:	
Information:	

IPR2025-00305
ASUS EX1002 Page 649

Total Files Size (in bytes):	19857

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IPR2025-00305
ASUS EX1002 Page 650

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

8791 7590 06/08/2012
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Connie Thayer	(Depositor's name)
Connie Thayer	(Signature)
September 7, 2012	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	12/07/2004	Luc Vantalon	6517P002	9254

TITLE OF INVENTION: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1740	$300	$0	$2040	09/10/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
AVERY, JEREMIAH L	2431	713-189000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Digital Keystone, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Mountain View, California

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 02-2666 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date September 7, 2012

Typed or printed name James C. Scheller Registration No. 31,195

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Docket No: 06517.P002 Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Luc Vantalon, et al.	Examiner: Avery, Jeremiah L.
Application No.: 11/007,116	Art Unit: 2431
Filing Date: December 7, 2004	
For: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER	Confirmation No. 9254
	Date of NOA: 06/08/2012

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Dear Sir:

Applicant is assuming that the Examiner's statement of reasons for allowance is to be taken in light of the structure and interaction recited in the claims. Applicant notes that the Examiner's comments may have paraphrased the language of the claims and it should be understood that the language of the claims themselves set out the scope of the claims.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: September 7, 2012

James C. Scheller
Reg. No. 31,195

1279 Oakmead Parkway
Sunnyvale, CA 94085
(408) 720-8300

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent and Trademark Office via electronic filing through the United States Patent and Trademark Electronic Filing System on:

September 7, 2012
Date of Deposit

Connie Thayer
Name of Person Filing Correspondence

Connie Thayer
Signature

9-7-12
Date

IPR2025-00305
ASUS EX1002 Page 652

Electronic Patent Application Fee Transmittal

Application Number:	11007116
Filing Date:	07-Dec-2004
Title of Invention:	METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
First Named Inventor/Applicant Name:	Luc Vantalon
Filer:	James Scheller Jr./Connie Thayer
Attorney Docket Number:	6517P002

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1740	1740
Publ. Fee- early, voluntary, or normal	1504	1	300	300

IPR2025-00305
ASUS EX1002 Page 653

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2040**

Electronic Acknowledgement Receipt	
EFS ID:	13692017
Application Number:	11007116
International Application Number:	
Confirmation Number:	9254
Title of Invention:	METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
First Named Inventor/Applicant Name:	Luc Vantalon
Customer Number:	8791
Filer:	James Scheller Jr./Connie Thayer
Filer Authorized By:	James Scheller Jr.
Attorney Docket Number:	6517P002
Receipt Date:	07-SEP-2012
Filing Date:	07-DEC-2004
Time Stamp:	20:48:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2040
RAM confirmation Number	7615
Deposit Account	022666
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

IPR2025-00305
ASUS EX1002 Page 655

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	06517P002_issue_fee_transmittal.pdf	99972 5e070bad71d7dcd5e622907cb04da0e5772d6218	no	1
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	06517P002_comments_on_allowance.pdf	36021 adac864e56e2a1b990af789bea62f7ffffe1ce0f	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31748 b2276268dc14339e0a2e89b073d9657de6f51025	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	167741		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/007,116	10/16/2012	8291236	6517P002	9254

8791 7590 09/26/2012

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 2005 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Luc Vantalon, Sunnyvale, CA;
Paolo Siccardo, Los Altos, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ACKNOWLEDGEMENT OF CHANGE TO SMALL ENTITY STATUS

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
11/007,116	12/07/2004	Luc Vantalon	6517P002	104092

The entity status change request below filed through Patent Center on 08/24/2023 has been accepted.

Certifications

APPLICANT ASSERTING SMALL ENTITY STATUS. See 37CFR 1.27.

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Lester J. Vincent/	Lester Vincent	31460

IPR2025-00305
ASUS EX1002 Page 658

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
11/007,116	**09/05/2023 04:42:24 PM ET**	**6517P002**

Title of Invention

METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	8291236
CONFIRMATION #	9254	FILED BY	Tyler Eller
PATENT CENTER #	62725261	FILING DATE	12/07/2004
CUSTOMER #	8791	FIRST NAMED INVENTOR	Luc Vantalon
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Levi Brown

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
22104-51 2023-09-01 3.73c Statement - VideoLabs.pdf	3	Assignee showing of ownership per 37 CFR 3.73	111 KB
22104-51 2023-09-01 VideoLabs Inc Power of Attorney.pdf	2	Power of Attorney	716 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
22104-51 2023-09-01 3.73c	73E66F75F8818671EA6130DF2E8C3AEBB9C8A36BD05F177C5

Statement - VideoLabs.pdf	C12EFD664FFEE993239DA381B9D89AA533A448747615CA644005D4F272947213FB80CF2FAADB4F5
22104-51 2023-09-01 VideoLabs Inc Power of Attorney.pdf	7E46DA38EEABA62E6FF2DD42FFD2A450CF7E24060D7930B1B3BF4262F1A7563678E8DD47C7A3093089A64F17092F0EE23C82950E6D79ED6F30ACA4458213F53B

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IPR2025-00305
ASUS EX1002 Page 660

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: VIDEOLABS, INC.

Application No./Patent No.: 8291236 Filed/Issue Date: October 16, 2012

Titled: METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER

VIDEOLABS, INC., a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Luc Vantalon et al. To: DIGITAL KEYSTONE, INC.

   The document was recorded in the United States Patent and Trademark Office at
   Reel 016072, Frame 0501, or for which a copy thereof is attached.

2. From: DIGITAL KEYSTONE, INC. To: VIDEOLABS, INC.

   The document was recorded in the United States Patent and Trademark Office at
   Reel 063555, Frame 0685, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Levi S. Brown/	September 1, 2023
Signature	Date
Levi S. Brown	72,533
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IPR2025-00305
ASUS EX1002 Page 663

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	11/007,116
Filing Date	December 7, 2004
First Named Inventor	Luc Vantalon
Title	METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER
Art Unit	2431
Examiner Name	JEREMIAH L AVERY
Attorney Docket Number	22104.51

SIGNATURE of Applicant or Patent Practitioner

Signature	/Levi S. Brown/	Date (Optional)	
Name	Levi S. Brown	Registration Number	72533
Title (if Applicant is a juristic entity)	Attorney for Applicant		
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IPR2025-00305
ASUS EX1002 Page 664

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 22913

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

VideoLabs, Inc.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	11/16/21
Name	Bill Goldman		
Title	SVP & Chief IP Officer		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IPR2025-00305
ASUS EX1002 Page 665

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/007,116	12/07/2004	Luc Vantalon	6517P002

CONFIRMATION NO. 9254

22913
Workman Nydegger
60 East South Temple
Suite 1000
Salt Lake City, UT 84111

POA ACCEPTANCE LETTER

OC000000061597295

Date Mailed: 09/11/2023

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 09/05/2023.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/kkdouglas/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/007,116	12/07/2004	Luc Vantalon	6517P002

CONFIRMATION NO. 9254

8791
WOMBLE BOND DICKINSON (US) LLP
ATTN: IP DOCKETING
P.O. Box 570489
ATLANTA, GA 30357-0037

POWER OF ATTORNEY NOTICE

OC000000061597113

Date Mailed: 09/11/2023

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 09/05/2023.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/kkdouglas/

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ACKNOWLEDGEMENT OF LOSS OF ENTITLEMENT TO ENTITY STATUS DISCOUNT

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
11/007,116	12/07/2004	Luc Vantalon	22104.51	124962

The entity status change request below filed through Patent Center on 11/09/2023 has been accepted.

Certifications

APPLICANT CHANGING TO REGULAR UNDISCOUNTED FEE STATUS

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Levi Brown/	Levi Brown	72533

IPR2025-00305
ASUS EX1002 Page 668