AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-113	3/31/2021	Eastern District of Texas

PLAINTIFF	DEFENDANT
KONINKLIJKE KPN N.V.	TELEFONAKTIEBOLAGET LM ERICSSON and ERICSSON INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	RE48,089	7/7/2020	KONINKLIJKE KPN N.V.
2	8,881,235	11/4/2014	KONINKLIJKE KPN N.V.
3	9,253,637	2/2/2016	KONINKLIJKE KPN N.V.
4	9,549,426	11/10/2020	KONINKLIJKE KPN N.V.
5	9,667,669	5/30/2017	KONINKLIJKE KPN N.V.

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
FINAL JUDGMENT FOR PLAINTIFF

CLERK	(BY) DEPUTY CLERK	DATE
David A. O'Toole	CH	9/7/22

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case 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 NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/139,433	11/04/2014	8881235	11-808-WO-US	1414

20306 7590 10/15/2014

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

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 206 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):

Frank Muller, Delft, NETHERLANDS;
Franklin Selgert, Berkel en Rodenrijs, NETHERLANDS;

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.

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)

20306 7590 07/03/2014
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

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.
13/139,433	08/15/2011	Frank Muller	11-808-WO-US	1414

TITLE OF INVENTION: SERVICE-BASED AUTHENTICATION TO A NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	10/03/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHAYANFAR, ALI	2493	726-003000

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 McDonnell Boehnen Hulbert
2 & Berghoff LLP
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)
Koninklijke KPN N.V.	The Hague, Netherlands
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO	Delft, Netherlands

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 credits any overpayment, to Deposit Account Number 13-2490 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Scott M. Miller/ Date October 1, 2014
Typed or printed name Scott M. Miller Registration No. 62,967

Samsung Ex. 1002, Page 3 of 341

Electronic Patent Application Fee Transmittal

Application Number:	13139433
Filing Date:	15-Aug-2011
Title of Invention:	SERVICE-BASED AUTHENTICATION TO A NETWORK
First Named Inventor/Applicant Name:	Frank Muller
Filer:	Scott Michael Miller
Attorney Docket Number:	11-808-WO-US

Filed as Large Entity

U.S. National Stage under 35 USC 371 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	960	960
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**960**

Electronic Acknowledgement Receipt

EFS ID:	20298972
Application Number:	13139433
International Application Number:	
Confirmation Number:	1414
Title of Invention:	SERVICE-BASED AUTHENTICATION TO A NETWORK
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	Scott Michael Miller
Filer Authorized By:	
Attorney Docket Number:	11-808-WO-US
Receipt Date:	01-OCT-2014
Filing Date:	15-AUG-2011
Time Stamp:	15:00:08
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$960
RAM confirmation Number	1350
Deposit Account	132490
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. 1.492 (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)

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	Post Allowance Communication - Incoming	11_808_WO_US_Comments.pdf	94244 217e8d3a866d3e3011c9af161d5950740e28e315	no	2
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	11_808_WO_US_Issue_Fee.pdf	89199 75374699dfe2b699b2cdb9121ac83edae6b6ce0f	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	32179 d4cd14d167130bc06a754c04e34273c5a326cfef	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	215622		

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
(Case No. 11-808-WO-US)

In the Application of:	)	
	)	
Frank Muller	)	
	)	**Examiner: Ali Shayanfar**
Serial No.: 13/139,433	)	
	)	**Art Unit: 2493**
Filed: August 15, 2011	)	
	)	**Confirmation No.: 1414**
Title: Service-Based Authentication To a Network	)	

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Dear Commissioner:

Applicant expresses appreciation for the Examiner's allowance of the present application. Applicant understands that the Examiner has thoroughly examined the claims and prior art of record and has concluded that the art of record, whether considered alone or in combination, fails to disclose or suggest the entirety of each combination of steps and/or structure recited by each of the allowed claims, that the Examiner has found each claim as a whole to patentably distinguish over the art of record, and that patentability of the claims does not necessarily rest on only any aspect that the Examiner listed in the statement of reasons for allowance.

Applicant takes no position regarding the Reasons for Allowance presented by the Examiner other than the positions Applicant may have previously taken during prosecution. Therefore, the Examiner's Reasons for Allowance should not be attributed to Applicant as a sole indication of the basis for Applicant's belief that the claims are patentable. Furthermore,

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, IL 60606
(312)913-0001

Applicant respectfully asserts that there may also be additional reasons for patentability of the claimed subject matter not explicitly stated in this record and Applicant does not waive its rights to such arguments by not further addressing such reasons herein.

Respectfully submitted,

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Date: October 1, 2014

By: /Scott M. Miller/
Scott M. Miller
Reg. No. 62,967

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, IL 60606
(312)913-0001

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

20306 7590 07/03/2014

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER
SHAYANFAR, ALI

ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 07/03/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/139,433	08/15/2011	Frank Muller	11-808-WO-US	1414

TITLE OF INVENTION: SERVICE-BASED AUTHENTICATION TO A NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	10/03/2014

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 ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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.

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)

20306 7590 07/03/2014
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

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.
13/139,433	08/15/2011	Frank Muller	11-808-WO-US	1414

TITLE OF INVENTION: SERVICE-BASED AUTHENTICATION TO A NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	10/03/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHAYANFAR, ALI	2493	726-003000

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 credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29
  NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27
  NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status.
  NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Samsung Ex. 1002, Page 11 of 341

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.
13/139,433	08/15/2011	Frank Muller	11-808-WO-US	1414

20306 7590 07/03/2014

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
SHAYANFAR, ALI	
ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 07/03/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

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.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B 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.

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.

Notice of Allowability	Application No. 13/139,433	Applicant(s) MULLER ET AL.	
	Examiner ALI SHAYANFAR	Art Unit 2493	AIA (First Inventor to File) Status No

-- 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 *6/17/2014*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
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 *1,3-9,11,12,14,16 and 18*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   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. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ 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).
6. ☐ 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. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/A. S./
Examiner, Art Unit 2493

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions.

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 June 18, 2014 has been entered.

2. Claims 1, 3-9, 12, 14, 16 and 18 are pending in the application.

Response to Arguments

3. Previous rejection of the pending claims over prior arts of record has been withdrawn in light of applicant's arguments and remarks filed on 06/17/2014.

4. In response to communications filed on 06/17/2014, the 112 rejection of claims 12 and 14 are withdrawn in view of the amendment. In regards to claim 12, examiner notes that based on applicant's specification Paragraph [0010] the terminal used in the method comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received. Therefore there is a corresponding hardware structure to terminal with hardware and processor which causes not invoking 112, 6th and therefore based on the above explanation there is no

112, 2nd rejections is required. In regards to claim 14, examiner notes that based on applicant's specification Paragraph [0026], "receiver configured to" and "generator configured to" has both structural and algorithm support.

Allowable Subject Matter

5. Claims 1, 3-9, 12, 14, 16 and 18 are allowed.

No reason for allowance is needed as the record is clear in light of applicant's arguments and amendment filed on 06/17/2014. See MPEP 1302.14(I).

6. None of the prior art of record, including the references cited in the Applicant's Information Disclosure Statement either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALI SHAYANFAR whose telephone number is (571)270-1050. The examiner can normally be reached on Monday through Friday 9:30-6:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Colin Carl can be reached on 571-272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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.

/A. S./
Examiner, Art Unit 2493
6/27/2014

/KAMBIZ ZAND/

Supervisory Patent Examiner, Art Unit 2434

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	((authenticat$ with response) with (depend$3) with (communication near channel)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/06/28 20:03
S1	174	((FRANK) near2 (MULLER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/10 22:49
S2	25	((FRANKLIN) near2 (SELGERT)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/10 22:49
S3	30	(determin$) near3 (type) near4 (channel connection) with (authentic$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:49
S4	9	(determin$3 detect$4 based) near3 (type) near4 (channel connection) with (authentic$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:50
S5	103	(determin$ detect$4 based) near3 (type) near4 (channel connection) with (authentic$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:51
S6	61	(determin$) near3 (type) near4 (channel connection) with (policy)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:51
S7	61	(determin$) near3 (type) near4 (channel connection) with (policy)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:52
S8	22	(determin$) near3 policy near3 (type) near4 (channel connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:52
S9	147	(determin$) near3 (policy authentic$) near3 (type) near4 (session channel connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:53
S10	6	(determin$) near3 (policy authentic$) near3 (type) near4 (session channel connection) near2 network$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:53
S11	3825	726/3.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:55
S12	28	Service-Based same Authentication same Network	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 23:52

Samsung Ex. 1002, Page 18 of 341

S13	606	(NEDERLANDSE ORGANISATIE VOOR TOEGEPAST).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/10 23:55
S14	1	S12 and S13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/10 23:55
S15	2	"20060288407"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/10 23:57
S16	2	"2005228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 01:59
S17	2	"2006288407"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:01
S18	2	"20060288407"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:02
S19	2	"2005228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:02
S20	3	"20050228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:03
S21	2	"20070283425"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 23:31
S22	183	AKA and RES and XRES and (authentication) and challenge	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/20 15:30
S24	86	AKA and RES and XRES and (authentication) and challenge and channel	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/20 15:30
S25	179	((FRANK) near2 (MULLER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/01/04 10:39
S26	118	((FRANKLIN) near2 (SELGERT)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/01/04 10:39
S27	118	((FRANKLIN) near2 (SELGERT)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:39
S28	43	(determin$) near3 (type) near4 (channel connection) with (authentic$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:39

Samsung Ex. 1002, Page 19 of 341

S29	10	(determin$3 detect$4 based) near3 (type) near4 (channel connection) with (authentic$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:39
S30	684	(NEDERLANDSE ORGANISATIE VOOR TOEGEPAST).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/04 10:39
S31	5681	726/3.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:40
S32	174	(determin$) near3 (policy authentic$) near3 (type) near4 (session channel connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:40
S33	17	(response) with (authentic$) same calculat$3 same (communication near channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:56
S34	2	(response) with (authentic$) same calculat$3 same (communication near channel) and (service near code)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:56
S35	15	(response) with (authentic$) same calculat$3 same (communication near channel) and (code)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 11:00
S36	3	"20050228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/04 11:08
S37	2	"20050228992" and calculat$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/04 11:08
S38	2	"20050228992" and calculat$4 and code	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/04 11:08
S39	312	(terminal device) same (moif$4 correct$4) same (authenticat$4) same information same channel	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 12:20
S40	59	(terminal device) same (moif$4 correct$4) same (authenticat$4 with information) same (communication near channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 12:21
S41	10	"authentication request" NEAR5 (includ$3 NEAR2 channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/05 15:25
S42	0	"authentication request" NEAR5 (includ$3 NEAR2 channel) and (service near code)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/07 23:43
S43	2	"13298704"	US-PGPUB; USPAT; USOCR	OR	OFF	2014/01/08 16:15

Samsung Ex. 1002, Page 20 of 341

S44	0	"13297226"	US-PGPUB; USPAT; USOCR	OR	OFF	2014/01/08 16:21
S45	0	"13297226"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/01/08 16:21
S46	6	"2005228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:20
S47	3	"20050228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:20
S48	11	"authentication request" with (includ$3 NEAR2 channel) and (calculat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:37
S49	32	"authentication request" with (communication NEAR2 channel) and (calculat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:43
S50	5	"authentication request" with (communication NEAR2 channel) same(calculat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:43
S51	0	calculat$ with (service near code) same "authentication request" same (includ$3 NEAR2 channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:14
S52	2	calculat$ with (service near code) same "authentication request" same (channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:14
S53	2	calculat$ with (code) same "authentication request" same (channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:14
S54	116	(authenticat$ near response) with (base$2 depend$3) same (channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:28
S55	12	(authenticat$ near response) with (depend$3) with (channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:28
S56	5	(authenticat$ near response) with (depend$3) with (communication near channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:29
S57	2	"20060288407" and terminal	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/11 13:28
S58	6	"20040068649"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/15 11:05

Samsung Ex. 1002, Page 21 of 341

S59	3	"7953846".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/15 11:13
S60	2	"20080211656"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/15 11:17
S61	6	"20040068649"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/15 11:27
S62	3	"20090174566"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/15 11:29
S63	3	"20130089200"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/15 14:28
S64	2	"20090292918"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/15 14:28
S65	184	((FRANK) near2 (MULLER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/06/18 23:05
S66	28	((FRANKLIN) near2 (SELGERT)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/06/18 23:05
S67	43	(determin$) near3 (type) near4 (channel connection) with (authentic$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/06/18 23:05
S68	6595	726/3.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/06/18 23:05
S69	748	(NEDERLANDSE ORGANISATIE VOOR TOEGEPAST).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/06/18 23:06
S70	11	"authentication request" with (includ$3 NEAR2 channel) and (calculat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/06/18 23:06
S71	6	"authentication request" with (includ$3 NEAR2 channel) and (calculat$3) and identifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/06/18 23:06
S72	5	(authenticat$ near response) with (depend$3) with (communication near channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/06/18 23:06
S73	16	(response) with (authentic$) same calculat$3 same (communication near channel) and (code)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/06/18 23:07
S75	78	(determin$) near3 (type) near4 (channel connection) with	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	2014/06/27 11:52

Samsung Ex. 1002, Page 22 of 341

		(policy)	JPO; DERWENT; IBM_TDB			
S76	1	"13139433"	US-PGPUB; USPAT; USOCR	OR	OFF	2014/06/28 18:32
S77	0	"13139433" and termina	US-PGPUB; USPAT; USOCR	OR	OFF	2014/06/28 18:32
S78	1	"13139433" and terminal	US-PGPUB; USPAT; USOCR	OR	OFF	2014/06/28 18:33

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	1	((authenticat$ with response) with (depend$3) with (communication near channel)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2014/06/28 20:04
L4	1	((service with code) with (authenticat$ with response) with (communication near channel)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2014/06/28 20:05
L6	11	((service with code) with (communication near channel) with terminal).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2014/06/28 20:06
L7	3	((service with code) with communication with channel with terminal with authenticat$4).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2014/06/28 20:07
S74	5052	726/3.ccls.	US-PGPUB; USPAT; UPAD	OR	ON	2014/06/18 23:07

6/ 28/ 2014 8:07:51 PM
C:\ Users\ ashayanfar\ Documents\ EAST\ Workspaces\ 13139433.wsp

Samsung Ex. 1002, Page 23 of 341

Anonymous usage of location-**based services through** spatial and temporal cloaking

M Gruteser, D Grunwald - ... on Mobile systems, applications and **services**, 2003 - dl.acm.org

... In an initial- ization phase, the nodes will set up an **authenticated** and encrypted connection with **...** Finally, the anonymity server forwards the message to the external **service**. **...** To be effective, the location anonymizer requires location-**based services** that are used with precise posi **...**

Cited by 1333 Related articles All 22 versions Cite Save

Secure **communications** over insecure **channels based** on short **authenticated** strings

S Vaudenay - Advances in cryptology–CRYPTO 2005, 2005 - Springer

... In particular, we do not consider denial-of-**services** attacks **...** 5 is depicted a SAS-**based** message **authentication** protocol **...** to **authenticate** in both directions and henceforth for **authenticated** key agreement as detailed in Appendix A. With weak **authentication channels**, the adversary **...**

Cited by 192 Related articles All 20 versions Cite Save

Enhancing security and privacy in biometrics-**based authentication** systems

NK Ratha, JH Connell, RM Bolle - IBM systems Journal, 2001 - ieeexplore.ieee.org

... one or more templates in the database, which could result either in authorizing a fraudulent individ- ual or denying **service** to the **...** A smartcard-**based ...** 8. Overriding the final decision: If the final match decision can be overridden by the hacker, then the **authentication** system has **...**

Cited by 1002 Related articles All 13 versions Cite Save

SPINS: Security protocols for sensor networks

A Perrig, R Szewczyk, JD Tygar, V Wen, DE Culler - Wireless networks, 2002 - dl.acm.org

... To prevent a potential denial-of-**service** (DoS) attack, where an attacker keeps sending bogus **...** verify that the corresponding MAC key was not yet disclosed by the base station (**based** on its **...** uses the key of the current interval, Ki, to compute the message **authentication** code (MAC **...**

Cited by 3809 Related articles All 142 versions Cite Save

... receiving requests from clients for specific formatted data **through** a default **channel** and establishing **communication through** separate control and data **channels**

DT Berry, JD Northcutt - US Patent 5,442,749, 1995 - Google Patents

... US5696901 *, May 24, 1996, Dec 9, 1997, Konrad; Allan M. Remote information **service** access system **based** on a client-server-**service** model. **...** Sextant Avionique, Method and device for distributing multimedia data, providing both video broadcast and video distribution **services**. **...**

Cited by 266 Related articles All 2 versions Cite Save

iMobile: a proxy-**based** platform for mobile **services**

CHH Rao, YFR Chen, MF Chen... - Proceedings of the first ..., 2001 - dl.acm.org

... iMobile introduces three abstractions on top of an agent-**based** proxy: devlets to interact with **...** to access multiple information spaces, and applets to implement application and **service** logic **...** maintains user and device profiles, which are used to provide personalized **services** and to **...**

Cited by 73 Related articles All 4 versions Cite Save

Authentication system **based** on periodic challenge/response protocol

DL Davis, L Smith - US Patent 6,088,450, 2000 - Google Patents

... Methods and devices enabling displays of electronic devices **based** on separation thereof. **...** 30, 2000, Sep 9, 2003, Telefonaktiebolaget Lm Ericsson (Publ), Terminal **authentication** procedure timing **...** and method for permitting only preregistered hardware to access a remote **service ...**

Cited by 196 Related articles All 2 versions Cite Save

Web-**based** biometric **authentication** system and method

MB Hoffberg, S Wong, YP Yu - US Patent 5,930,804, 1999 - Google Patents

... to cost/benefit trade-offs, entities offering Web information, **services** and other **...** eg, the **authentication** center 24 enrolls individuals and provides an **authentication service** respecting its **...** exhaustion: (i) the **authentication** station 24 does not support **authentication based** on biometric **...**

Cited by 200 Related articles All 3 versions Cite Save

Authentication process including setting up a secure **channel** between a subscriber and a **service** provider accessible **through** a telecommunications operator

MJP Wary - US Patent 6,745,326, 2004 - Google Patents

... Mutual **authentication** is **based** on the operator distributing a value R1 at the time that the **...** The operator guarantees the quality of the scheme for **authentication** and confidentiality **services**. **...** If the **service** provider obtains a value identical to the value of R3 received from the **...**

Cited by 54 Related articles All 2 versions Cite Save

Flexible interface to **authentication services** in a distributed data processing environment

LK Loucks, TA Smith - US Patent 5,481,720, 1996 - Google Patents

... "Kerberos: An **Authentication Service** For Open Network **...** These above two references are herein incorporated by reference. This Kerberos **based** remote **authentication** authenticates users working at one node in a distributed data processing system to **services** running on **...**

Cited by 131 Related articles All 2 versions Cite Save

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13139433	MULLER ET AL.
	Examiner	Art Unit
	ALI SHAYANFAR	2493

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	3	3/10/2013	AS
726	3	1/4/2014	AS
726	3 (Updated)	6/18/2014	AS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search and Assignee search	3/10/2013	AS
EAST Text search: determine, type, channel, connection, authenticate, authentication, policy, XRES, XSC, service request, RES, cryptography	3/10/2013	AS
NPL: Google scholar:Service-Based Authentication to a Network	3/10/2013	AS
Inventor search and Assignee search	1/4/2014	AS
EAST Text search: determine, type, channel, connection, authenticate, authentication, policy, XRES, XSC, service request, RES, cryptography, request, communication channel	1/4/2014	AS
NPL: Google scholar: Service-Based Authentication to a Network	1/4/2014	AS
Inventor search and Assignee search (Updated)	6/18/2014	AS
EAST text search: See the attached history (Updated)	6/18/2014	AS
NPL: Google scholar: Service-Based Authentication to a Network	6/18/2014	AS

INTERFERENCE SEARCH

/A.S./ Examiner.Art Unit 2493	

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
726	3	6/18/2014	AS

/A.S./ Examiner.Art Unit 2493	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13139433	MULLER ET AL.
	Examiner	**Art Unit**
	ALI SHAYANFAR	2493

CPC						
Symbol					**Type**	**Version**
H04W		12	/	06	F	2013-01-01
H04L		63	/	1466	I	2013-01-01
H04W		88	/	06	A	2013-01-01
H04L		63	/	0853	I	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

/A.S./ Examiner.Art Unit 2493	06/28/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	13	
/KAMBIZ ZAND/ Supervisory Patent Examiner.Art Unit 2434	06/29/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13139433	MULLER ET AL.
	Examiner	**Art Unit**
	ALI SHAYANFAR	2493

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
726	3	H	0	4	L	29 / 06 (2006.01.01)						

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

/A.S./ Examiner.Art Unit 2493	06/28/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	13	
/KAMBIZ ZAND/ Supervisory Patent Examiner.Art Unit 2434	06/29/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13139433	MULLER ET AL.
	Examiner	**Art Unit**
	ALI SHAYANFAR	2493

☐ 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	1		17												
	2	13	18												
2	3														
3	4														
4	5														
5	6														
6	7														
7	8														
8	9														
	10														
9	11														
10	12														
	13														
11	14														
	15														
12	16														

/A.S./ Examiner.Art Unit 2493	06/28/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	13	
/KAMBIZ ZAND/ Supervisory Patent Examiner.Art Unit 2434	06/29/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	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

BIB DATA SHEET

CONFIRMATION NO. 1414

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/139,433	08/15/2011 RULE	726	2493	11-808-WO-US

APPLICANTS

INVENTORS

Frank Muller, Delft, NETHERLANDS;
Franklin Selgert, Berkel en Rodenrijs, NETHERLANDS;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/EP09/67201 12/15/2009

**** FOREIGN APPLICATIONS ***************************

EUROPEAN PATENT OFFICE (EPO) 08021705.2 12/15/2008

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

08/18/2011

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/ALI SHAYANFAR/ Examiner's Signature	☐ Initials	NETHERLANDS	5	18	5

ADDRESS

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606
UNITED STATES

TITLE

Service-Based Authentication to a Network

FILING FEE RECEIVED		
1550	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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13139433	MULLER ET AL.
	Examiner	**Art Unit**
	ALI SHAYANFAR	2493

✓	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	03/10/2013	01/04/2014	06/27/2014						
1	1	✓	✓	=						
	2	✓	-	-						
2	3	✓	✓	=						
3	4	✓	✓	=						
4	5	✓	✓	=						
5	6	✓	✓	=						
6	7	✓	✓	=						
7	8	✓	✓	=						
8	9	✓	✓	=						
	10	✓	-	-						
9	11	✓	✓	=						
10	12	✓	✓	=						
	13	✓	-	-						
11	14	✓	✓	=						
	15	✓	-	-						
12	16	✓	✓	=						
	17	✓	-	-						
13	18	✓	✓	=						

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. 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 contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13/139,433	Filing Date	2011-08-15	Docket Number (if applicable)	11-808-WO-US	Art Unit	2493
First Named Inventor	Frank Muller			Examiner Name	Ali Shayanfar		

This is a Request for Continued Examination (RCE) under 37 CFR 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. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 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).

☐ 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.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 132490

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. 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 contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Scott M. Miller/	Date (YYYY-MM-DD)	2014-06-17
Name	Scott M. Miller	Registration Number	62967

This collection of information is required by 37 CFR 1.114. 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.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

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 the Freedom of Information Act requires disclosure of these records.

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 inspections 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.

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. 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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 11-808-WO-US

Application Number: 13/139,433

Filed: August 15, 2011

For: Service-Based Authentication To A Network

Art Unit: 2493

Examiner: Ali Shayanfar

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600
☐	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

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

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 13-2490.

☐ Payment made via EFS-Web.

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.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 62,967.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Scott M. Miller/ — Signature

June 17, 2014 — Date

Scott M. Miller — Typed or printed name

312-913-0001 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 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.

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
(Case No. 11-808-WO-US)

In the Application of:	)	
	)	
Frank Muller	)	
	)	**Examiner: Ali Shayanfar**
Serial No.: 13/139,433	)	
	)	**Art Unit: 2493**
Filed: August 15, 2011	)	
	)	**Confirmation No.: 1414**
Title: Service-Based Authentication To a Network	)	

Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

RESPONSE TO OFFICE ACTION MAILED JANUARY 17, 2014

Dear Sir:

In response to the office action mailed January 17, 2014, Applicant submits the following amendments and remarks. Amendments to the claims begin at page 2, and remarks begin at page 8.

Along with this response, Applicant is submitting a request for continued examination (RCE) and a request for a two-month extension of time, along with the requisite fees. Applicant believes that no other fees are required at this time. However, please charge any underpayment or credit any overpayment to Deposit Account No. 132490. Further, Applicant generally authorizes the Office to treat any filing in this matter that requires an extension of time as incorporating a request for such an extension.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

AMENDMENTS TO THE CLAIMS

1. (Currently amended) Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising:

- the terminal sending a service request for access to a network service;
- the terminal receiving in response to the service request an authentication request from the network;
- the terminal identifying the communication channel through which the authentication request was received;
- the terminal determining a service code associated with the identified communication channel; and
- the terminal sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the determined service code, thereby securely including information regarding the ~~identity~~ identified ~~of the~~ communication channel through which the authentication request was received into the response.

2. (Canceled)

3. (Previously presented) Method according to claim 1, wherein the terminal comprises an identity module and a service interface (SI) module configured to securely

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

communicate with the identity module and to identify the communications channel through which the authentication request was received.

4. (Currently amended) Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising the steps of:

- the terminal modifying the authentication information on the basis of the identified communications channel; and
- the terminal generating the authentication response on the basis of the modified authentication information.

5. (Currently amended) Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising:

- the terminal generating the authentication response;
- the terminal modifying the authentication response on the basis of the identified communications channel.

6. (Previously presented) Method according to claim 1, the method further comprising:

- the terminal sending a service request via a predetermined communications channel to the network;
- the network generating an expected service code on the basis of the type of communications channel the service request was sent to the network; and
- determining on the basis of the expected service code an expected response.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

7. (Previously presented) Method according to claim 6, the method further comprising:

- comparing the expected response with the authentication response sent by the terminal to the network; and
- determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.

8. (Previously presented) Method according to claim 1, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

9. (Currently amended) Service interface module for use in a terminal, the service interface module comprising:

- a receiver configured to receive an authentication signal from the network via one of the communications interfaces of the terminal;
- a channel identifier configured to identify the communication channel through which the authentication signal was received and provide a service code associated with the identified communication channel;
- a channel interface configured to establish a secure communication channel between the module and an identity module of the terminal[[,]]; and

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

– a modifier configured to modify an authentication response of the identity module on the basis of [[a]] the service code [[of]] associated with the identified communication channel.

10. (Canceled)

11. (Currently amended) An identity module for establishing a safe communication channel with a service interface module as claimed in claim 9, the identity module comprising: a calculator for calculating a response upon receipt of an authentication request; and a modifier for modifying the response on the basis of a predetermined mathematical function using a service code [[of]] associated with the identified communication channel.

12. (Currently amended) A terminal for accessing network services, the terminal comprising (i) an operating system having memory configured to store program instructions and (ii) a service interface module configured to identify a communication channel through which an authentication request is received, wherein the program instructions are executable by the terminal ~~configured~~ to:

- receive an authentication request from the network;

- determine the communication channel through which the authentication request is received;

- determine a service code associated with the ~~type of~~ identified communication channel via which the authentication request was received by the terminal; and

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

- send in response to an authentication request a modified response to the network wherein the modification depends on the determined service code.

13. (Canceled)

14. (Currently amended) A network node for service-based authentication of a terminal to a network, the network node ~~configured to~~ comprising:

- a receiver configured to receive an authentication data request; [[and]]

- a first generator configured to determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network; and

- a second generator configured to generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code.

15. (Canceled)

16. (Previously presented) A system for service based authentication to a network, comprising:

- a terminal configured to receive an authentication request from the network, to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal, and

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

to send in response to the authentication request a modified response to the network, wherein the modification depends on the determined service code;

- a network node configured to receive an authentication data request and determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and configured to generate in response to the receipt of the authentication data request a modified expected response wherein the expected response depends on the determined expected service code and configured to compare the modified response with the modified expected response.

17. (Canceled)

18. (Previously presented)A computer program product comprising software code portions configured for, when run in the memory of a terminal, executing the method according to claim 1.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

REMARKS

1. Summary of the Office Action

In the office action mailed January 17, 2014, the Examiner: (i) rejected claims 12 and 14 under 35 U.S.C. § 112, first paragraph as allegedly failing to comply with the enablement requirement and under 35 U.S.C. § 112, second paragraph as allegedly failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention; (ii) rejected claims 1, 3-6, 8-9, 12, 14, 16 under 35 U.S.C. § 103(a) as allegedly being obvious over U.S. Patent Application Pub. No. 2006/0288407 (Naslund) in view of U.S. Patent Application Pub. No. 2006/0148483 (Howard); (iii) rejected claim 7 under 35 U.S.C. § 103(a) as allegedly being obvious over Naslund in view of Howard in view of the Ericsson reference ("How to mitigate the interleaving attack and reduce the trust in the Authenticator (S3-030084)", 3GPP TCG SA WG3 SECURITY); and (iv) rejected claim 11 under 35 U.S.C. § 103(a) as allegedly being obvious over Naslund in view of Howard in view of U.S. Patent Application Pub. No. 2005/008695 (Sheth).

2. Status of the Claims

Pending are claims 1, 3-9, 11-12, 14, 16 and 18, of which claims 1, 9, 12, 14, and 16 are independent and the remainder are dependent.

Applicant has amended claims 1, 9, 11-12, and 14 to clarify the invention. Support for these claim amendments is found throughout the specification. For instance, support for the amendment to claim 12 is found throughout the specification including, for instance, at page 3, lines 22-27, page 3, lines 4-7, page 9, lines 8-14, and page 10, lines 11-19. Further, support for the amendment to claim 14 is found throughout the specification including, for instance, at page 6, lines 29-36. Still further, support for the amendments to claims 1 and 11 is found throughout

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

the specification. Yet still further, support for the amendment to claim 9 is found throughout the specification including, for instance, at page 5, lines 19-21. Applicant has also amended claims 4-5 for matters of form.

Applicant reserves the right to pursue in a continuation application the subject matter of any of the claims without the present amendments, and any other subject matter disclosed by this application.

3. Response to Rejection under 35 U.S.C. § 112, first and second paragraphs

As mentioned above, the Examiner rejected claims 12 and 14 under 35 U.S.C. § 112, first paragraph as allegedly failing to comply with the enablement requirement, and the Examiner rejected claims 12 and 14 under 35 U.S.C. § 112, second paragraph as allegedly failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

In particular, the Examiner stated that "[a] single means claim, i.e., where a means recitation does not appear in combination with another recited element of means, is subject to an undue breadth rejection under 35 U.S.C. 112, first paragraph." (Office action, page 3.) Further, the Examiner stated that "[a]fter considering the claim as a whole and in view of Applicant's disclosure the scope of the term 'terminal configured to:' and network node configured to:' are unclear because claims cites 'terminal or network node without reciting a structure to define the bounds of the claims. Appropriate correction is required." (*Id.* at page 4.)

Applicant does not acquiesce in the rejections. Nonetheless, to expedite prosecution, Applicant has amended claims 12 and 14 to clarify the invention. Applicant notes that these amended claims are clearly not single means claims.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

In view of these amendments, Applicant respectfully submits that the rejection of claims 12 and 14 under 35 U.S.C. § 112, first paragraph is moot. Applicant therefore respectfully requests withdrawal of the 35 U.S.C. § 112, first paragraph rejection. Further, in view of these amendments, Applicant respectfully submits that the rejection of the claims under 35 U.S.C. § 112, second paragraph is moot. Applicant therefore respectfully requests withdrawal of the 35 U.S.C. § 112, second paragraph rejection.

4. Response to Rejections under 35 U.S.C. § 103

As noted above, the Examiner rejected claims 1, 3-6, 8-9, 12, 14, 16 as allegedly being obvious over Naslund in view of Howard, rejected claim 7 as allegedly being obvious over Naslund in view of Howard in view of the Ericsson reference, and rejected claim 11 as allegedly being obvious over Naslund in view of Howard in view of Sheth. Of these claims, claims 1, 9, 12, 14, and 16 are independent. Applicant addresses these independent claims in the following subsections.

i. Claim 1

Applicant has amended claim 1 to clarify that the terminal performs the method step of sending an authentication response to the network, and further that the response which is calculated on the basis of the information in the authentication request and the determined service code, now securely includes information regarding the identified communication channel through which the authentication request was received into the response. This is the same communication channel identified by the terminal as the communication channel through which the authentication request is received.

In the office action, the Examiner appeared to admit that Naslund does not disclose (i) the feature of "the terminal determining a service code associated with the identified communication

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

channel" nor (ii) the feature (which Applicant has currently amended) of "the terminal sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the service code, thereby securely including information regarding the identified communication channel through which the authentication request was received into the response." (*See* office action, page 6.) However, the Examiner provided reasoning that these features are instead provided by Howard. (*Id.*) In making this assertion, the office action refers to text supplied in the abstract and in paragraphs [0007] and [0110]-[0111] of Howard. (*Id.* at pages 6-7.)

The office action argues that, in the case of the first of the two missing features, Howard discloses a terminal which determines a service code associated with the identified communication channel because, in the view of the office action, Howard describes that the contents of the authentication response signal received in the channel depend on the 'context' of the authentication request signal. (*Id.*) This, according to the office action, is described in the abstract. Applicant has studied Howard in detail and respectfully disagrees with this interpretation of Howard.

Applicant has searched Howard for an explanation of what is meant by 'context' and cannot find one. Indeed, Applicant cannot even find the term 'context' appearing anywhere else in Howard and can find no explanation of what it might mean in Howard. However, Applicant has examined the text in paragraphs [0110]-[0111] and finds that they appear to correspond to the part of the abstract which includes the term 'context'. In particular, paragraphs [0110]-[0111] describe the prior art situation in which the contents of an authentication response signal depends on the random number included in the authentication request signal, paragraph [0111] lines 1-10.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

In Applicant's view, paragraph [0111] discloses simply that the contents of the disclosed authentication response signal depends on the **content** of the authentication request signal which preceded it. Applicant can find no other disclosure in Howard that contradicts this interpretation.

In view of this realization, Applicant respectfully wonders if the term 'context' as written in the abstract might actually be a typographic error, and should in fact be written as 'content'. If this is indeed the case, then in Applicant's view the text of the abstract is fully consistent with paragraphs [0110]-[0111].

In view of this, Applicant is of the view that the abstract clearly does not disclose a service code. Further, even if a view is taken that there is no typographic error in the abstract and that the word "context" in the abstract is in fact not a typographical error, then Applicant still finds no mention of a 'service code' anywhere in Howard, nor anything that can be described as a service code as recited in the claim. A 'context', as currently written in the abstract, which Applicant would assume, if it were correct, to mean the general technological context or background to the authentication request signal, is not the same as a service code as recited in the claim. Notably, the service code described in the claim is associated with an identified communication channel and is a determinable code actually identifiable within the terminal. However, there is no such determinable code disclosed in Howard.

In light of the above, Howard fails to disclose the feature of "the terminal determining a service code associated with the identified communication channel." Therefore, Howard fails to overcome the deficiency of Naslund. Since Howard does not make up for the deficiency of Naslund, combining the references together would not reasonably or logically result in the invention of claim 1. Consequently, for at least this reason, the rejection of claim 1 should be withdrawn, and the claim should be allowed.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Further, Howard fails to disclose the claim feature of "the terminal sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the service code, thereby securely including information regarding the identified communication channel through which the authentication request was received into the response." The office action argues that this second missing feature is also disclosed in Howard, paragraphs [0007] and [0110]-[0111]. (*See* office action, pages 6-7.)

In making this rejection, the office action presents the reasoning that paragraph [0007] discloses allocating a unique channel to each terminal and receiving an authentication response signal, the contents of which depend on the context. (*Id.*) Applicant has studied paragraph [0007] and cannot find a reference to 'context'. The Office action further presents the reasoning that paragraphs [0110]-[0111] disclose securely including identification of the communication channel in the authentication response. (*Id.* at page 7.)

However, at best, Howard discloses in paragraphs [0007] and [0110]-[0111] an ordinary authentication arrangement as already known in the state of the art and in particular there is no inclusion of information regarding the identification of the channel. Instead, paragraph [0111] at best describes that "[t]he MES 2 operates on the random number using a code or key stored within the MES 2….". Notably, this merely describes the operation of authentication in the prior art, whereby an authentication challenge includes a random number which the terminal, in this case MES, manipulates using an authentication key. An authentication key is sometimes referred to as a code, which is normally shorthand for 'code word'. Applicant notes that the code referred to in this sense is a mathematical formulation and not a "service code" as recited in claim 1. As

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

is known in the art, authentication keys are specific to a terminal, not a type of communication channel and further there is no disclosure in paragraph [0111] that the code or key in any way describes the type of channel. Rather, it simply discloses that the code or key is specific to the MES, paragraph [0111], lines 6-8, further indicating to Applicant that what is described is a normal authentication procedure as already known to the person of ordinary skill in the art.

The "service code" of claim 1, however, is associated with the identified communication channel, which as Applicant understands, is acknowledged by the Examiner to mean the *type* of communication channel. (*See* office action page 6, lines 4-7.) The service code is therefore determined based on the type of communication channel through which the authentication request is received. Further, in Applicant's view, paragraphs [0110]-[0111] do not show use of an authentication key or code which is determined based on the type of communication channel and, similarly, Applicant finds no disclosure that Howard shows that the type of communication channel is encoded into the authentication response. As explained, Applicant finds that Howard merely seems to show the provision of a normal authentication response using the known key methods.

Meanwhile, use of the method of claim 1 allows an indication of the type of communication channel through which an authentication request was received at a terminal to be then incorporated into the authentication response in order to counter the problem of man-in-the-middle attacks to a mobile terminal, as explained, for example, on page 2, line 30, to page 3, line 2, of Applicant's specification.

In light of the above, Howard fails to disclose the feature of "the terminal sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

information in the authentication request and the service code, thereby securely including information regarding the identified communication channel through which the authentication request was received into the response." Therefore, Howard fails to overcome the deficiency of Naslund. Since Howard does not make up for the deficiency of Naslund, combining the references together would not reasonably or logically result in the invention of claim 1. Consequently, for at least this reason as well, the rejection of claim 1 should be withdrawn, and the claim should be allowed.

In light of the above, the invention of claim 1 would not have reasonably or logically followed from the combination of the cited references. Thus, Applicant submits that claim 1 is allowable. Furthermore, Applicant submits that claims 3-8 and 18 are allowable as well for at least the reason that they each depend from allowable claim 1.

ii. Claim 9

In the rejection of claim 9, the office action refers to paragraphs [0004], [0034]-[0035], [0065] and [0084]. (*See* office action, pages 11-12.)

Claim 9 has been amended to include the feature that the channel identifier also provides a service code associated with the identified communication channel.

Applicant has studied the cited paragraphs and believes they do not disclose the added feature. Further, for the reasons already explained above, Applicant believes this feature is not disclosed anywhere in Howard. In particular, Applicant has studied paragraph [0084] and is of the view that, while this paragraph shows that the terminal can detect if an authentication request is received through different types of channels, it proposes an alternative solution to the solution proposed in the independent claims, and in particular claim 9. Paragraph [0084] discloses that when the terminal detects that a channel of different technological type is used that the terminal

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

undertakes extra security procedures, for example by rerouting the request to a security enhancing application. But paragraph [0084] does not disclose the solution proposed in the claims of providing "a service code associated with the identified communication channel."

Applicant therefore believes claim 9 is patentable over the combination of Naslund and Howard. Thus, Applicant respectfully submits that claim 9 is allowable. Further, Applicant submits that claim 11 is allowable as well for at least the reason that it depends from allowable claim 9.

iii. Claim 12

In the rejection of claim 12, the office action uses substantially equivalent reasoning to that used against claim 1, and further presents the reasoning that paragraph [0084] discloses receipt of an authentication data request. (*See* office action, pages 13-14.) In Applicant's view paragraph [0084] appears to show receipt of an authentication request but further, Applicant would like to point out that further examination of paragraph [0084] indicates that while it shows that the terminal can detect if an authentication request is received through different types of channels, it proposes an alternative solution to the solution proposed in the independent claims, and in particular claim 12. Paragraph [0084] discloses that when the terminal detects that a channel of different technological type is used that the terminal undertakes extra security procedures, for example by rerouting the request to a security enhancing application. But paragraph [0084] does not disclose the solution proposed in the claims of determining a service code associated with the identified communication channel and calculating the authentication response based on this service code.

Therefore, Applicant believes claim 12 is patentable over the combination of Naslund and Howard. Thus, Applicant respectfully submits that claim 12 is allowable.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

iv. Claim 14

In the rejection of claim 14, the office action has proposed equivalent reasoning to that proposed in the rejection of claim 12 and correspondingly Applicant believes that the arguments raised with respect to claim 12 apply also to claim 14. Applicant therefore believes that claim 14 is patentable over the combination of Naslund and Howard. Thus, Applicant respectfully submits that claim 14 is allowable.

v. Claim 16

In the rejection of claim 16, the office action has proposed equivalent reasoning to that proposed in the rejection of claim 12 and correspondingly Applicant believes that the arguments raised with respect to claim 12 apply also to claim 16. Applicant therefore believes claim 16 is also patentable over the combination of Naslund and Howard. Thus, Applicant respectfully submits that claim 16 is allowable.

vi. Claims 7 and 11

Claim 7 was rejected under 35 USC 103(a) over Naslund in view of Howard in view of the Ericsson reference. Claim 7 is dependent upon claim 6 which is itself dependent upon claim 1, which is allowable for the reasons already given. Ericsson, as previously argued, does not cure the deficiency of Howard and Naslund. Claim 7 is therefore believed by Applicant to be patentable over the combination of Naslund, Howard and Ericsson.

Claim 11 was rejected under 35 USC 103(a) over Naslund in view of Howard in view of Sheth. Claim 11 has been amended to clarify that the service code is associated with the identified communication channel. In the rejection of claim 11, the office action presents reasoning that Naslund and Howard disclose the features of claim 11 with the exception only of the calculator and the modifier. For the reasons already given, Applicant disagrees and believes

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

that neither Naslund nor Howard disclose the determination of the service code associated with the identified communication channel, as described in claim 9, referenced by claim 11, and described also now in claim 11. Further, Sheth does not cure the deficiency of either Naslund or Howard.

Applicant is therefore of the view that claim 11 is patentable over the combination of Naslund, Howard and Sheth.

5. Conclusion

For the foregoing reasons, Applicant submits that claims are allowable. Therefore, Applicant requests favorable reconsideration and allowance of the claims.

Applicant does not acquiesce in any assertion in the office action that is not expressly addressed by these remarks.

Should the Examiner wish to discuss this case with the undersigned, the Examiner is invited to call the undersigned at (312) 913-3350.

Respectfully submitted,

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Date: June 17, 2014

By: /Scott M. Miller/
Scott M. Miller
Reg. No. 62,967

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Electronic Patent Application Fee Transmittal

Application Number:	13139433
Filing Date:	15-Aug-2011
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	Scott Michael Miller/Lisa Panatera
Attorney Docket Number:	11-808-WO-US

Filed as Large Entity

U.S. National Stage under 35 USC 371 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 - 2 months with $0 paid	1252	1	600	600

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for Continued Examination	1801	1	1200	1200
		Total in USD ($)		**1800**

Electronic Acknowledgement Receipt

EFS ID:	19325916
Application Number:	13139433
International Application Number:	
Confirmation Number:	1414
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	Scott Michael Miller
Filer Authorized By:	
Attorney Docket Number:	11-808-WO-US
Receipt Date:	17-JUN-2014
Filing Date:	15-AUG-2011
Time Stamp:	14:56:15
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1800
RAM confirmation Number	1232
Deposit Account	132490
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. 1.492 (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)

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)	11-808-WO-US_RCE.pdf	79173 a6fe4dfb698b9218ec4f01c17d84ef54d993a343	no	3
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2	Extension of Time	11-808-WO-US_extension.pdf	152691 4f5bae0428989994435a700e49af00f185693589	no	2
Warnings:					
Information:					
3	Amendment Submitted/Entered with Filing of CPA/RCE	11-808-WO-US_response.pdf	149546 291d38e2514cb93f4bb515a7a9014e96f13a2f22	no	18
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32324 6fac641bef4f5f67fbe2e9eca8949c51a90fdc35	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	413734		

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.
13/139,433	08/15/2011	Frank Muller	11-808-WO-US	1414

20306 7590 01/17/2014

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
SHAYANFAR, ALI	

ART UNIT	PAPER NUMBER
2493	

MAIL DATE	DELIVERY MODE
01/17/2014	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. 13/139,433	Applicant(s) MULLER ET AL.	
	Examiner ALI SHAYANFAR	Art Unit 2493	AIA (First Inventor to File) Status No

-- 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 MONTHS 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 *9/26/2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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) *1,3-9,11,12,14,16 and 18* 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, 3-9, 11-12,14, 16 and 18* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ 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).

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).

Certified copies:

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)).

** 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) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

Response to Arguments

2. This is a reply to the application filed on 9/26/2013, in which, claims 1, 3-9, 11,12,14,16 and 18 are pending. Claims 1, 3-9, 11-12, 14, 16 and 18 are amended. Claims 2, 10, 13, 15 and 17 have been canceled.

3. In response to communications filed on 9/26/2013, the applicant's arguments in regards to the claims 1-18 have been considered but moot in view of the new ground(s) of rejection necessitated by Applicant's amendment to the claims.

However the newly "Howard et al" (Publication No. 2006/0148483, hereinafter Howard) discloses the limitation that applicant argued as below:

Howard discloses a method for authenticating terminals in a wireless communication "*service involves receiving registration requests from terminals requiring access, transmitting to each of the terminals a signaling channel assignment signal allocating a duplex signaling channel uniquely to each terminal, transmitting in the signaling channel an authentication request signal, receiving an authentication response signal in the channel, the contents of which depend on the context of the authentication request signal, and deciding whether to allow access to the system according to the contents of the authentication response signal*"

4. Applicant's argument in regard to 101 rejections of claims 1, 2, 4-5 and 9-10 has been considered and persuasive. Therefore the rejections of the claims 1, 2, 4-5 and 9-10 are withdrawn based on applicant's amendment.

5. Applicant's argument in regard to 112 (first Paragraph) is considered but not persuasive. Therefore the rejections of the claims 12 and 14 are maintained.

Claim Rejections - 35 USC § 112

6. The following is a quotation of 35 U.S.C. 112(a):
(a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), first paragraph:
The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 12 and 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

A single means claim, i.e., where a means recitation does not appear in combination with another recited element of means, is subject to an undue breadth rejection under 35 U.S.C. 112, first paragraph. *In re Hyatt*, 708 F.2d 712, 714-715, 218 USPQ 195, 197 (Fed. Cir. 1983) (A single means claim which covered every conceivable means for achieving the stated purpose was held nonenabling for the scope of the claim because the specification disclosed at most only those means known

to the inventor.). When claims depend on a recited property, a fact situation comparable to *Hyatt* is possible, where the claim covers every conceivable structure (means) for achieving the stated property (result) while the specification discloses at most only those known to the inventor. Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of 35 U.S.C. 112(b):

(B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 12 and 14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Claims 12 and 14 recites the limitation "terminal configured to:" and “network node configured to: receive authentication data request from the network. After considering the claim as a whole and in view of Applicants’ disclosure the scope of the term "terminal configured to:" and “network node configured to:” are unclear because claims cites “terminal or network node without reciting a structure to define the bounds of the claims. Appropriate correction is required.

Claim Rejections - 35 USC § 103

11. 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.

12. Claims 1, 3-6, 8-9, 12, 14 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naslund et al (Publication No. 2006/0288407, hereinafter Naslund) [Applicant's IDS] in view of Howard et al (Publication No. 2006/0148483, hereinafter Howard)

As to claim 1Naslund discloses a method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network **(Naslund, Figure, 4, illustrates a user terminal, such as a mobile phone or a personal computer, which generally has some form of network communication capabilities such as GSM, Bluetooth)**, the method comprising:

the terminal sending a service request for access to a network service **(Naslund, Paragraph [0003] discloses communications in GSM, UMTS is triggered as a response to an access request; UMTS letting the network interact with this device through a user terminal in a**

challenge-response protocol); the terminal receiving in response to the service request an authentication request from the network **(Naslund, Paragraph [0084] discloses AKA request)**; the terminal identifying the communication channel through which the authentication request was received **(Naslund, Paragraph [0084] the terminal (mobile) may be configured to determine whether the AKA request initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces)**; Naslund does not discloses the terminal determining a service code associated with the identified communication channel, sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the service code, thereby securely including information regarding the identity of the communication channel through which the authentication request was received into the response. Howard discloses the terminal determining a service code associated with the identified communication channel **(Howard, Abstract, receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal)** and, sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the service code **(Howard, Abstract, Paragraph [0007] discloses receiving registration request from terminal and transmitting allocating unique signaling channel to each terminal and receiving**

an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal; Paragraphs [0110-011] the MES-specific signaling channel, the LES 14 transmits a `challenge` packet in the form of a header and a random number. The MES 2 operates on the random number using a code or key stored within the MES 2, such as on a smart card, and transmits the result of the operation in the MES-specific signaling channel.), thereby securely including information regarding the identity of the communication channel through which the authentication request was received into the response. **(Howard, Abstract, Paragraph [0007] discloses the unique channel or channels is used for an authentication transaction with the wireless terminal prior to allowing calls to be set up with that terminal; Paragraph [0111] discloses The LES 14 performs the same operation using a copy of the code or key specific to that MES 2, the copy being stored securely within the LES 14, and compares the result of the operation with that transmitted by the MES 2)** It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of Howard by showing sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the service code, thereby securely including information regarding the identity of the communication channel through which the authentication request was received into the response as taught by Howard in order provide unique channel for an authentication transaction with the wireless terminal.

As to claim 3 Naslund in view of Howard discloses method according to claim 1, wherein the terminal comprises an identity module and a service interface (SI) module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received **(Naslund, Paragraph [0003] discloses many network services are based on storing user credentials on a tamper-resistant "security device", e.g. a GSM SIM (Subscriber Identity Module), a UMTS SIM or an ISIM (IP Multimedia SIM) card, and letting the network interact with this device through a user terminal in a challenge-response protocol to perform (subscriber) Authentication and Key Agreement (AKA).**

As to claim 4 Naslund in view of Howard discloses method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising: the terminal modifying the authentication information on the basis of the identified communications channel; the terminal generating, the authentication response on the basis of the modified authentication information **(Naslund, Paragraph [0004] In a subscriber database/authentication center, commonly referred to as an AuC in the context of mobile communication systems, an expected response XRES is generated based on knowledge of the secret key and a generated challenge RAND. The AKA protocol may, and typically will, involve an AAA (Authorization, Authentication and Accounting) server, which may or may not be**

physically co-located with the AuC. The challenge RAND and the expected response XRES are normally transferred to the AAA server. The challenge is sent to the terminal ME (Mobile Equipment), which assisted by the security device computes the response RES. The response is sent back to the AAA server, and if it matches the expected response, the user is authenticated)

As to claim 5 Naslund in view of Howard discloses a method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising: the terminal generating, the authentication response; and the terminal modifying, the authentication response on the basis the identified communications channel **(Naslund, Paragraph [0099] Regardless of the terminal type the SIM is attached to, and the way the SIM is accessed [by Bluetooth, IRDA, in card-reader, etc.] all AKA related processing takes place on the SIM, including the security enhancing steps. The enhanced security processing may involve manipulation of output parameters and/or input parameters of the AKA process, as schematically illustrated for a general tamper-resistant security device in FIG. 10.)**

As to claim 6 Naslund in view in view of Howard discloses a method according to claim 1, the method further comprising:

the terminal sending a service request via a predetermined communications channel to the network **(Howard, Abstract, authenticating terminals in a wireless**

communication service involves receiving registration requests from terminals requiring access, transmitting to each of the terminals a signaling channel assignment signal allocating a duplex signaling channel uniquely to each terminal); the network generating an expected service code on the basis of the type of communications channel the service request was sent to the network; and determining on the basis of expected service code an expected response. **(Howard, Abstract, Paragraph [0007] discloses receiving registration request from terminal and transmitting allocating unique signaling channel to each terminal and receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal; Paragraphs [0110-011] the MES-specific signaling channel, the LES 14 transmits a `challenge` packet in the form of a header and a random number. The MES 2 operates on the random number using a code or key stored within the MES 2, such as on a smart card, and transmits the result of the operation in the MES-specific signaling channel.)**

As to claim 8 Naslund in view of Howard discloses a method according to claim 1, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface. **(Naslund, Paragraph [0085] another example of a security policy suitable for implementation in a tamper-resistant security device of the invention is related to the existing proposals for enhancing the security of the**

3GPP Gb interface; Paragraph [0084] Paragraph [0084] the terminal [mobile] may be configured to determine whether the AKA request initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces)

As to claim 9 Naslund discloses a service interface module for use in a terminal, the service interface module comprising: a receiver configured to receive an authentication signal from the network via one of the communications interfaces of the terminal **(Naslund, Paragraph [0084] discloses AKA request; the invention to maintain the overall security even if a tamper-resistant security device such as a SIM is used in an insecure environment or when reusing the AKA protocol over a less secure interface Paragraph [0004])**; a channel identifier configured to identifying the communication channel through which the authentication signal was received, **(Naslund, Paragraph [0084] the terminal (mobile) may be configured to determine whether the AKA request initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces)**; a channel interface configured to establish a secure communication channel between the module and an identity module of the terminal. **(Naslund, Paragraph [0034] A main merit is that the solution is future proof and easy to administer in a secure way by authenticated downloads. [0035] the solution is in a sense transparent to the device into which the tamper-resistant security device is plugged. In addition, it enables secure remote access directly to the security**

device, such as a SIM, when the security device is still in the original (mobile) terminal, communicating over e.g. Bluetooth)

Naslund does not disclose preferably by providing a service code associated with the identified communication channel and a modifier configured to modify an authentication response of the identity module on the basis of a service code of the identified communication channel. Howard disclose preferably by providing a service code associated with the identified communication channel **(Howard, Abstract, receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal)** a modifier configured to modify an authentication response of the identity module on the basis of a service code of the identified communication channel **(Howard, Paragraph [0065] discloses the SAP handler is set up according to Quality of Service parameters [service code] supplied in the call set-up message, but in the case of a locally initiated call these parameters may be modified if the remote party signals that some of the Quality of Service parameters are not accepted)** It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of Howard by showing a service code associated with the identified communication channel and a modifier configured to modify an authentication response of the identity module on the basis of a service code of the identified communication channel as taught by Howard in order provide unique channel for an authentication transaction with the wireless terminal.

As to claim 12 Naslund in view of ERICSSON discloses a terminal, for accessing network services, the terminal configured to:

receive authentication data request **(Naslund, Paragraph [0084] discloses AKA request)** Naslund does not discloses determining an expected service code associated with the type of communication channel via which the authentication data request was received by the network and generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code. Howard discloses determining an expected service code associated with the type of communication channel via which the authentication data request was received by the network **(Howard, Abstract, receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal)** and generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code **(Howard, Abstract, Paragraph [0007] discloses receiving registration request from terminal and transmitting allocating unique signaling channel to each terminal and receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal; Paragraphs [0110-011] the MES-specific signaling channel, the LES 14 transmits a `challenge` packet in the form of a header and a random number. The MES 2 operates on the random number using a code or key stored within the MES 2, such as on a smart**

card, and transmits the result of the operation in the MES-specific signaling channel.) It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of Howard by showing determining an expected service code associated with the type of communication channel via which the authentication data request was received by the network and generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service codeas taught by Howard in order provide unique channel for an authentication transaction with the wireless terminal.

As to claim 14 Naslund in view of Howard discloses a network node for service-based authentication of a terminal to a network, the network node configured to: receive authentication data request **(Naslund, Paragraph [0084] discloses AKA request)** Naslund does not discloses determining an expected service code associated with the type of communication channel via which the authentication data request was received by the network and generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code. Howard discloses determining an expected service code associated with the type of communication channel via which the authentication data request was received by the network **(Howard, Abstract, receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication**

request signal) and generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code **(Howard, Abstract, Paragraph [0007] discloses receiving registration request from terminal and transmitting allocating unique signaling channel to each terminal and receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal; Paragraphs [0110-011] the MES-specific signaling channel, the LES 14 transmits a `challenge` packet in the form of a header and a random number. The MES 2 operates on the random number using a code or key stored within the MES 2, such as on a smart card, and transmits the result of the operation in the MES-specific signaling channel.)** It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of Howard by showing determining an expected service code associated with the type of communication channel via which the authentication data request was received by the network and generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service codeas taught by Howard in order provide unique channel for an authentication transaction with the wireless terminal.

As to claim 16 Naslund discloses a system for service based authentication to a network, the system comprising:

a terminal configured to receive an authentication request from the network **(Naslund, Paragraph [0084] discloses AKA request)** Naslund does not discloses determine service code associated with the type of communication channel via which the authentication data request was received by terminal and to send in response to the receipt of an authentication request a modified response to network, wherein the modification of the expected response depends on the determined expected service code; network node configured to receive an authentication data request and determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and configured to generate in response to the receipt of the authentication data request a modified expected response wherein the expected response depends on the determined expected service code and configured to compare the modified response with the modified expected response.

Howard discloses determine service code associated with the type of communication channel via which the authentication data request was received by terminal **(Howard, Abstract, receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal)** and to send in response to the receipt of an authentication request a modified response to network, wherein the modification of the expected response depends on the determined expected service code **(Howard, Abstract, Paragraph [0007] discloses receiving registration request from terminal and transmitting allocating unique signaling channel to each terminal and**

receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal; Paragraphs [0110-011] the MES-specific signaling channel, the LES 14 transmits a `challenge` packet in the form of a header and a random number. The MES 2 operates on the random number using a code or key stored within the MES 2, such as on a smart card, and transmits the result of the operation in the MES-specific signaling channel.); network node configured to receive an authentication data request and determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network **(Howard, Abstract, receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal)** and configured to generate in response to the receipt of the authentication data request a modified expected response wherein the expected response depends on the determined expected service code and configured to compare the modified response with the modified expected response**(Howard, Paragraph [0065] discloses the SAP handler is set up according to Quality of Service parameters [service code] supplied in the call set-up message, but in the case of a locally initiated call these parameters may be modified if the remote party signals that some of the Quality of Service parameters are not accepted)** It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of Howard by showing determine service code associated with the type of communication channel via which the authentication data request was

received by terminal and to send in response to the receipt of an authentication request a modified response to network, wherein the modification of the expected response depends on the determined expected service code; network node configured to receive an authentication data request and determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and configured to generate in response to the receipt of the authentication data request a modified expected response wherein the expected response depends on the determined expected service code and configured to compare the modified response with the modified expected response as taught by Howard in order provide unique channel for an authentication transaction with the wireless terminal.

139. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naslund et al (Publication No. 2006/0288407, hereinafter Naslund) [Applicant's IDS] in view of Howard et al (Publication No. 2006/0148483, hereinafter Howard) further in view of (ERICSSON: "How to mitigate the interleaving attack and reduce the trust in the Authenticator (S3-030084)" 3GPP TCG SA WG3 SECURITY, Hereinafter ERICSSON) [Applicant's IDS]

As to claim 7 Naslund in view of Howard discloses all the elements in the claim above except comparing the expected response with the authentication response send by the terminal to the network; and determining the terminal to be in an un-trusted

state if the authentication response is not equal to the expected response. ERICSSON discloses comparing the expected response with the authentication response send by the terminal to the network; and determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response **(ERICSSON, Page 2, lines7-8, shows authenticator checks that RES=XRES and that the A-Data-MAC is correct)** It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of Howard further in view of ERICSSON by showing comparing the expected response with the authentication response send by the terminal to the network; and determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response as taught by ERICSSON in order to mitigated the interleaving attack and reduce the trust in authenticator.**(Page2, ERICSSON)**

14. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naslund et al (Publication No. 2006/0288407, hereinafter Naslund) [Applicant's IDS] in view of Howard et al (Publication No. 2006/0148483, hereinafter Howard) further in view of Sheth et al (Publication No. 2005/008695, hereinafter Sheth)

As to claim 11 Naslund in view of Howard discloses all the elements in the claim above except a calculator for calculating a response upon receipt of an authentication request; and, a modifier for modifying the response on the basis of a predetermined mathematical function using a service code on the identified communication channel.

Sheth discloses calculator for calculating a response upon receipt of an authentication request; and, a modifier for modifying the response on the basis of a predetermined mathematical function using a service code on the identified communication channel **(Sheth, Paragraph [0047] discloses PPP authentication request including a virtual channel ID [service code] is received by an AAA server or similar device. A determination is made regarding whether a domain configuration override attribute exists in a virtual circuit profile associated with the DSLAM port used to receive the PPP session; Paragraph [0065] calculator to determine whether the service associated with the virtual circuit matches the service associated with a domain configuration override attribute)** It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of Howard further in view of Sheth by showing calculator for calculating a response upon receipt of an authentication request; and, a modifier for modifying the response on the basis of a predetermined mathematical function using a service code on the identified communication channel as taught by Sheth in order to prevents unauthorized PPP sessions from being forwarded to a destination **(Sheth, Paragraph [0019])**

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US. Publication No. : 2009/0103728 A1 Patel discloses a method and system for secure wireless communications. In particular, the present invention relates to a method

of establishing authentication keys at both the network and mobile equipment in order to establish a mutually authenticated communication channel.

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).

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.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALI SHAYANFAR whose telephone number is (571)270-1050. The examiner can normally be reached on Monday through Friday 9:30-6:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Colin Carl can be reached on 571-272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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.

/A. S./
Examiner, Art Unit 2493
1/04/2014

/CARL COLIN/

Supervisory Patent Examiner, Art Unit 2493

Notice of References Cited	Application/Control No. 13/139,433	Applicant(s)/Patent Under Reexamination MULLER ET AL.	
	Examiner ALI SHAYANFAR	Art Unit 2493	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0148483	07-2006	Howard et al.	455/450
*	B	US-2005/0086495	04-2005	Sheth et al.	713/182
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	174	((FRANK) near2 (MULLER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/10 22:49
S2	25	((FRANKLIN) near2 (SELGERT)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/10 22:49
S3	30	(determin$) near3 (type) near4 (channel connection) with (authentic$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:49
S4	9	(determin$3 detect$4 based) near3 (type) near4 (channel connection) with (authentic$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:50
S5	103	(determin$ detect$4 based) near3 (type) near4 (channel connection) with (authentic$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:51
S6	61	(determin$) near3 (type) near4 (channel connection) with (policy)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:51
S7	61	(determin$) near3 (type) near4 (channel connection) with (policy)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:52
S8	22	(determin$) near3 policy near3 (type) near4 (channel connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:52
S9	147	(determin$) near3 (policy authentic$) near3 (type) near4 (session channel connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:53
S10	6	(determin$) near3 (policy authentic$) near3 (type) near4 (session channel connection) near2 network$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:53
S11	3825	726/3.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:55
S12	28	Service-Based same Authentication same Network	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 23:52
S13	606	(NEDERLANDSE ORGANISATIE VOOR TOEGEPAST).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/10 23:55

Samsung Ex. 1002, Page 84 of 341

S14	1	S12 and S13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/10 23:55
S15	2	"20060288407"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/10 23:57
S16	2	"2005228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 01:59
S17	2	"2006288407"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:01
S18	2	"20060288407"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:02
S19	2	"2005228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:02
S20	3	"20050228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:03
S21	2	"20070283425"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 23:31
S22	183	AKA and RES and XRES and (authentication) and challenge	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/20 15:30
S24	86	AKA and RES and XRES and (authentication) and challenge and channel	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/20 15:30
S25	179	((FRANK) near2 (MULLER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/01/04 10:39
S26	118	((FRANKLIN) near2 (SELGERT)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/01/04 10:39
S27	118	((FRANKLIN) near2 (SELGERT)).INV.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:39
S28	43	(determin$) near3 (type) near4 (channel connection) with (authentic$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:39
S29	10	(determin$3 detect$4 based) near3 (type) near4 (channel connection) with (authentic$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:39

Samsung Ex. 1002, Page 85 of 341

S30	684	(NEDERLANDSE ORGANISATIE VOOR TOEGEPAST).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/04 10:39
S31	5681	726/3.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:40
S32	174	(determin$) near3 (policy authentic$) near3 (type) near4 (session channel connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:40
S33	17	(response) with (authentic$) same calculat$3 same (communication near channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:56
S34	2	(response) with (authentic$) same calculat$3 same (communication near channel) and (service near code)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 10:56
S35	15	(response) with (authentic$) same calculat$3 same (communication near channel) and (code)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 11:00
S36	3	"20050228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/04 11:08
S37	2	"20050228992" and calculat$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/04 11:08
S38	2	"20050228992" and calculat$4 and code	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2014/01/04 11:08
S39	312	(terminal device) same (moif$4 correct$4) same (authenticat$4) same information same channel	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 12:20
S40	59	(terminal device) same (moif$4 correct$4) same (authenticat$4 with information) same (communication near channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/04 12:21
S41	10	"authentication request" NEAR5 (includ$3 NEAR2 channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/05 15:25
S42	0	"authentication request" NEAR5 (includ$3 NEAR2 channel) and (service near code)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/07 23:43
S43	2	"13298704"	US-PGPUB; USPAT; USOCR	OR	OFF	2014/01/08 16:15
S44	0	"13297226"	US-PGPUB; USPAT; USOCR	OR	OFF	2014/01/08 16:21
S45	0	"13297226"	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	OFF	2014/01/08 16:21

Samsung Ex. 1002, Page 86 of 341

			JPO; DERWENT; IBM_TDB			
S46	6	"2005228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:20
S47	3	"20050228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:20
S48	11	"authentication request" with (includ$3 NEAR2 channel) and (calculat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:37
S49	32	"authentication request" with (communication NEAR2 channel) and (calculat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:43
S50	5	"authentication request" with (communication NEAR2 channel) same(calculat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 19:43
S51	0	calculat$ with (service near code) same "authentication request" same (includ$3 NEAR2 channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:14
S52	2	calculat$ with (service near code) same "authentication request" same (channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:14
S53	2	calculat$ with (code) same "authentication request" same (channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:14
S54	116	(authenticat$ near response) with (base$2 depend$3) same (channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:28
S55	12	(authenticat$ near response) with (depend$3) with (channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:28
S56	5	(authenticat$ near response) with (depend$3) with (communication near channel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/01/10 20:29

EAST Search History (Interference)

<This search history is empty>

1/11/2014 12:30:54 PM
C:\Users\ashayanfar\Documents\EAST\Workspaces\13139433.wsp

Samsung Ex. 1002, Page 87 of 341

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13139433	MULLER ET AL.
	Examiner	**Art Unit**
	ALI SHAYANFAR	2493

✓	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	03/10/2013	01/04/2014	01/04/2014						
	1	✓	✓							
	2	✓	-							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	-							
	11	✓	✓							
	12	✓	✓							
	13	✓	-							
	14	✓	✓							
	15	✓	-							
	16	✓	✓							
	17	✓	-							
	18	✓	✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13139433	MULLER ET AL.
	Examiner	Art Unit
	ALI SHAYANFAR	2493

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	3	3/10/2013	AS
726	3 (Updated)	1/4/2014	

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search and Assignee search	3/10/2013	AS
EAST Text search: determine, type, channel, connection, authenticate, authentication, policy, XRES, XSC, service request, RES, cryptography	3/10/2013	AS
NPL: Google scholar:Service-Based Authentication to a Network	3/10/2013	AS
Inventor search and Assignee search (Updated)	1/4/2014	AS
EAST Text search: determine, type, channel, connection, authenticate, authentication, policy, XRES, XSC, service request, RES, cryptography, request, communication channel(Updated).	1/4/2014	AS
NPL: Google scholar: Service-Based Authentication to a Network	1/4/2014	AS

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/A.S./ Examiner.Art Unit 2493	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
(Case No. 11-808-WO-US)

In the Application of:	)	
	)	
Frank Muller	)	
	)	**Examiner: Ali Shayanfar**
Serial No.: 13/139,433	)	
	)	**Art Unit: 2493**
Filed: August 15, 2011	)	
	)	**Confirmation No.: 1414**
Title: Service-Based Authentication To a Network	)	

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

RESPONSE TO OFFICE ACTION MAILED APRIL 1, 2013

Dear Sir:

In response to the office action mailed April 1, 2013, Applicant submits the following amendments and remarks. Amendments to the claims begin at page 2, and remarks begin at page 6.

Along with this response, Applicant is submitting a request for a three-month extension of time, along with the requisite fee. Applicant believes that no other fees are required at this time. However, please charge any underpayment or credit any overpayment to Deposit Account No. 132490. Further, Applicant generally authorizes the Office to treat any filing in this matter that requires an extension of time as incorporating a request for such an extension.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Amendments to the Claims

1. (Currently Amended) Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising:

- the terminal sending a service request for access to a network service;
- the terminal receiving in response to the service request an authentication request from the network;
- the terminal identifying the communication channel through which the authentication request was received; [[and,]]
- the terminal determining a service code associated with the identified communication channel; and
- sending an authentication response ~~RES~~ to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the service code, thereby securely including information regarding the identity of the communication channel through which the authentication request was received into the response.

2. (Canceled)

3. (Currently Amended) Method according to claim 1, wherein the terminal comprises an identity module and a service interface (SI) module~~, the SI preferably implemented as a trusted hardware module,~~ configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.

4. (Currently Amended) Method according to claim 1, wherein the authentication request comprises authentication information~~, preferably a random challenge RAND,~~ the method further comprising ~~the steps of~~:

- the terminal modifying the authentication information on the basis of the identified communications channel; and
- the terminal generating~~, preferably using an authentication and key agreement (AKA) of a telecommunication standard,~~ [[an]] the authentication response [[RES]] on the basis of the modified authentication information.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

5. (Currently Amended) Method according to claim 1, wherein the authentication request comprises authentication information~~, preferably a random challenge RAND,~~ the method further comprising:

- the terminal generating~~, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication standard, an~~ the authentication response[[RES]]; and
- the terminal modifying~~, preferably using a one-way function,~~ the authentication response ~~parameter RES~~ on the basis the identified communications channel.

6. (Currently Amended) Method according to claim 1 [[2]], the method further comprising:

- the terminal sending a service request via a predetermined communications channel to the network;
- the network generating an expected service code [[XSC]] on the basis of the type of communications channel the service request was sent to the network; and
- determining, on the basis of the expected service code, [[XSC]] an expected response [[XRES]].

7. (Currently Amended) Method according to claim 6, the method further comprising:

- comparing the expected response [[XRES]] with the authentication response [[RES]] [[send]] sent by the terminal to the network; and
- determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.~~RES is not equal to XRES.~~

8. (Previously Presented) Method according to claim 1, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

9. (Currently Amended) Service interface module for use in a terminal, ~~preferably configured to securely process all authentication information transmitted to and from an identity module in the terminal,~~ the service interface module comprising:

- a receiver configured to receive ~~for receiving~~ an authentication signal from the network via one of the communications interfaces of the terminal;
- a channel identifier configured to identify ~~for identifying~~ the communication channel through which the authentication signal was received~~, preferably by providing a service code associated with the identified communication channel~~;

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

- a channel interface configured to establish ~~for establishing~~ a secure communication channel between the module and an identity module of the terminal,
- a modifier configured to modify an authentication response of the identity module on the basis of a service code of the identified communication channel.

10. (Canceled)

11. (Currently Amended) An identity module~~, preferably a smartcard,~~ for establishing a safe communication channel with a service interface module as claimed in claim 9, the identity module comprising: a calculator for calculating a response ~~RES – preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA –~~ upon receipt of an authentication request; and~~, optionally,~~ a modifier for modifying the response [[RES]] on the basis of a predetermined mathematical function using ~~information on~~ a service code of the identified communication channel.

12. (Currently Amended) A terminal~~, preferably a mobile device,~~ for accessing network services, the terminal configured to:

- receive an authentication request from the network;

- determine a service code associated with the type of communication channel via which the authentication request was received by the terminal; and

- send in response to an authentication request a modified response [[RES']] to the network wherein the modification depends on the determined service code ~~type of communication channel the authentication request was received by the terminal~~.

13. (Canceled)

14. (Currently Amended) A network node for service-based authentication of a terminal to a network, the network node configured to:

- receive an authentication data request and

- determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network; and

- generate in response to the receipt of an authentication data request a modified expected response [[XRES']], wherein the modification of the expected response [[XRES]] depends on the determined expected service code ~~the type of communication channel the authentication data response was sent to the network~~.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

15. (Canceled)

16. (Currently Amended) A system for service based authentication to a network, the system comprising:

- a terminal configured to receive an authentication request from the network, to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal, and
  ~~a terminal configured~~ to send in response to ~~an~~ the authentication request a modified response [[RES']] to the network, wherein the modification depends on the determined service code ~~the type of communication channel the authentication request was received by the terminal~~;
- a network node configured to receive an authentication data request and determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and configured to generate in response to the receipt of ~~an~~ the authentication data request a modified expected response [[XRES']] wherein the expected response depends on the determined expected service code and configured to compare the modified response with the modified expected response~~RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network~~.

17. (Canceled)

18. (Currently Amended)A computer program product comprising software code portions configured for, when run in the memory of a terminal, ~~preferable a mobile device,~~ executing the method according to claim 1.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Remarks

1. Summary of the Office Action

In the office action mailed April 1, 2013, the Examiner: (i) objected to claims 1-2; (ii) rejected claims 1, 2, 4-5, and 9-10 under 35 U.S.C. § 101 as being allegedly directed to non-statutory subject matter; (iii) rejected claims 12 and 14 under 35 U.S.C. § 112, first paragraph as allegedly failing to comply with the enablement requirement; (iv) rejected claims 2-5, 9, and 11-12 under 35 U.S.C. § 112, second paragraph as allegedly failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention; (v) rejected claims 1, 3-5, 8, 14 and 18 under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent Application Pub. No. 2006/0288407 (Naslund); and (vi) rejected claims 2, 6-7, 9-13, 15-17 under 35 U.S.C. § 103(a) as allegedly being obvious over Naslund in view of the Ericsson reference.

2. Status of the Claims

Applicant has amended claims 1, 3-7, 9, 11-12, 14, and 16 to clarify the invention. Support for these claim amendments is found throughout the specification. Further, Applicant has canceled claims 2, 10, 13, 15, and 17.

As a result, pending are claims 1, 3-9, 11-12, 14, 16, and 18, of which claims 1, 9, 12, 14, and 16 are independent and the remainder are dependent.

Applicant reserves the right to pursue in a continuation application the subject matter of any of the claims without the present amendments, and any other subject matter disclosed by this application.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

3. Response to Objection to the Claims

As noted above, the Examiner objected to claims 1-2 because they include reference characters which are not enclosed within parentheses. In particular, the Examiner noted that "[i]n claims 1-2, 'RES' should have parentheses." (Office action, page 2.) Applicant has amended claim 1 to overcome the Examiner's objection. Further, Applicant has canceled claim 2. For these reasons, Applicant respectfully requests withdrawal of the objection to the claims.

4. Response to Rejection under 35 U.S.C. § 101

As mentioned above, the Examiner rejected claims 1, 2, 4-5, and 9-10 as being allegedly directed to non-statutory subject matter. Of these claims, claims 1 and 9 are independent.

Independent claim 1 as now amended recites (i) the terminal sending a service request for access to a network service, (ii) the terminal receiving in response to the service request an authentication request from the network, (iii) the terminal identifying the communication channel through which the authentication request was received, (iv) the terminal determining a service code associated with the identified communication channel, and (v) sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the service code, thereby securely including information regarding the identity of the communication channel through which the authentication request was received into the response. These steps are clearly machine implementations and thus meet the test for statutory subject matter set forth by the Federal Circuit in the *Bilski* case. Therefore, claim 1 is directed to statutory subject matter, and claims 4-5 are directed to statutory subject matter due to their dependency from independent claim 1.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Claim 9 as amended recites, *inter alia*, the elements of (i) a receiver configured to receive an authentication signal from the network via one of the communications interfaces of the terminal, (ii) a channel identifier configured to identify the communication channel through which the authentication signal was received, (iii), a channel interface configured to establish a secure communication channel between the module and an identity module of the terminal, and (iv) a modifier configured to modify an authentication response of the identity module on the basis of a service code of the identified communication channel. Applicant respectfully submits that claim 9 recites articles or objects that constitute a machine or manufacture within the meaning of 35 U.S.C. 101. For instance, Applicant believes that the text on page 12, line 21 to page 13, line 10 makes clear that claim 9 does not address non-statutory subject matter.

For these reasons, Applicant respectfully requests withdrawal of the 35 U.S.C. § 101 rejections.

5. Response to Rejection under 35 U.S.C. § 112, first paragraph

As mentioned above, the Examiner rejected claims 12 and 14 under 35 U.S.C. § 112, first paragraph as allegedly failing to comply with the enablement requirement.

Applicant notes that claim 12 is directed to a terminal for accessing network services. Applicant has amended claim 12 to clarify that the terminal is configured to (i) receive an authentication request from the network, (ii) determine a service code associated with the type of communication channel via which the authentication request was received by the terminal, and (iii) send in response to an authentication request a modified response to the network wherein the modification depends on the determined service code.

Further, Applicant notes that claim 14 is directed to a network node for service-based authentication of a terminal to a network. Applicant has amended claim 14 to clarify that the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

network node is configured to (i) receive an authentication data request, (ii) determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network, and (ii) generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code.

In view of these amendments, Applicant respectfully submits that the rejection of claims 12 and 14 under 35 U.S.C. § 112, first paragraph is moot. Applicant therefore respectfully requests withdrawal of the 35 U.S.C. § 112, first paragraph rejection.

6. Response to Rejection under 35 U.S.C. § 112, second paragraph

As noted above, the Examiner rejected claims 2-5, 9, and 11-12 under 35 U.S.C. § 112, second paragraph as allegedly failing to particularly point out and distinctly claim the subject matter which the applicant regards as his invention. Applicant has amended claims 3-5, 9, and 11-12 to clarify the invention. Further, Applicant has canceled claim 2.

In view of these amendments, Applicant respectfully submits that the rejection of the claims under 35 U.S.C. § 112, second paragraph is moot. Applicant therefore respectfully requests withdrawal of the 35 U.S.C. § 112, second paragraph rejection.

7. Response to Rejections under 35 U.S.C. §§ 102 and 103

As noted above, the Examiner rejected claims 1, 3-5, 8, 14 and 18 as allegedly being anticipated by Naslund, and the Examiner rejected claims 2, 6-7, 9-13, 15-17 as allegedly being obvious over Naslund in view of the Ericsson reference. Of these claims, claims 1, 9, 12, 14, and 16 are independent. Applicant addresses these independent claims in the following subsections.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

i. Claim 1

Applicant has amended claim 1 to include the features of claim 2. The Examiner rejected claim 2 as being allegedly obvious over Naslund in view of Ericsson. Applicant submits that the Examiner clearly erred in rejecting claim 2 as being obvious over Naslund in view of Ericsson. In particular, Applicant submits that the Examiner clearly erred in reaching this conclusion of obviousness, because combining the references together would not reasonably or logically result in the invention of claim 2.

In the office action, the Examiner stated that Ericsson discloses "determining a service code associated with the identified communication channel; calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including . . . information regarding the identity of the communication channel through which the authentication request was received into the response." (Office action, page 12.) This assertion appears to be based on an interpretation of Ericsson disclosing a service identifier Sld in Solution 2, which is used in a modified challenge, and that the USIM calculates both RES and A-data-MAC. (*See* office action, page 12.)

Applicant has studied Ericsson and disagrees with this interpretation of the disclosure. While Ericsson discloses in Solution 2 the use of a service identifier Sld to generate derived XRESd, there is little explanation given about what is meant by this service identifier and no explanation which suggests it corresponds to a service code as described in claim 1. Further, there is no disclosure of how the service code is determined and therefore no disclosure that the service identifier Sld is associated with a communication channel through which a authentication request has been received.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

The only explanation that Applicant can find regarding service identifier Sld is on page 2, last line of Solution 2, where Ericsson states that "[t]he UE determines the Sld to be used on the intended service." However, this explanation is unclear and Applicant notes that there are several possibilities for interpretation. For instance, Sld could refer to an intended or preferred communication channel for an outgoing message or could refer to a preferred network to carry a call. Alternatively, Sld could refer to a type of service, for example differentiating between voice call service, SMS service, or voicemail service. Still alternatively, Sld may refer to the communication channel which the terminal should use to communicate back to the base station or network node.

Correspondingly, Applicant believes it cannot be assumed that service identifier Sld refers to a service code associated with an identified communication channel through which an authentication request is received. This interpretation can simply not be derived from the disclosure of Ericsson. Further, while Ericsson discloses calculating both RES and A-data-MAC, neither of these are explicitly disclosed as including any reference to a service code associated with an identified communication channel.

In contrast, claim 2 recites that a service code is determined for the communication channel through which the authentication request is received and that a response is calculated on the basis of the service code.

Naslund also fails to disclose determination of a service code associated with a communication channel through which an authentication request is received and calculation of the response on the basis of the service code. Therefore, these features cannot be produced from a combination of Naslund and Ericsson.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

In light of the above, the combination of the cited references would not reasonably or logically result in the invention of claim 2. Thus, the Examiner has not established *prima facie* obviousness of claim 2 under M.P.E.P. § 2142, and therefore, the Examiner erred in rejecting claim 2 based on the Naslund/Ericsson combination. Since claim 1 now incorporates the subject matter of claim 2, Applicant submits that claim 1 is allowable. Furthermore, Applicant submits that claims 3-8 are allowable as well for at least the reason that they each depend from allowable claim 1.

ii. Claim 9

Applicant has amended claim 9 to recite, *inter alia*, the element of "a modifier configured to modify an authentication response of the identity module on the basis of a service code of the identified communication channel." Applicant submits that, for at least reasons similar to the reasons discussed above with respect to claim 1, the invention of claim 9 would not reasonably or logically follow from the teachings of the cited art, and thus Applicant submits that claim 9 is allowable. In particular, as Applicant argued above in support of claim 1, the feature of an authentication response modified on the basis of a service code of the identified communication channel is simply not disclosed in either Ericsson or Naslund. Therefore, neither Ericsson nor Naslund discloses a modifier configured to perform this action.

Further, Applicant submits that claim 11 is allowable as well for at least the reason that it depends from allowable claim 9.

iii. Claim 12

Claim 12 recites, *inter alia*, that the terminal is configured to (i) receive an authentication request from the network, (ii) determine a service code associated with the type of communication channel via which the authentication request was received by the terminal, and

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

(iii) send in response to an authentication request a modified response to the network wherein the modification depends on the determined service code. Applicant submits that, for at least the reasons discussed above with respect to claim 1, the invention of claim 12 would not reasonably or logically follow from the teachings of the cited art, and thus Applicant submits that claim 12 is allowable.

iv. Claim 14

Claim 14 recites, *inter alia*, that the network node is configured to (i) receive an authentication data request, (ii) determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network, and (iii) generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code. Applicant submits that, for at least the reasons discussed above with respect to claim 1, the invention of claim 14 would not reasonably or logically follow from the teachings of the cited art, and thus Applicant submits that claim 14 is allowable.

v. Claim 16

In the rejection of claim 16, the Office Action presents reasoning that Naslund in view of Ericsson discloses determination of a service code associated with the type of communication channel via which the authentication request was received by the terminal and that this is shown in Naslund, paragraphs [0120]-[0121]. (*See* office action, pages 19-20.) Applicant has studied these paragraphs and can find no such disclosure, as these paragraphs appears to teach only that AKA output parameters Kc and/or RES can be combined into possibly longer output parameters Kc'and RES'. However, nowhere in paragraphs [0120]-[0121], nor elsewhere in Naslund, can Applicant find disclosure of determination of a service code associated with the type of

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

communication channel via which the authentication request was received by the terminal. In light of the above (and in view of comments above in support of claim 1), the invention of claim 16 would not reasonably or logically follow from the teachings of the cited art. Thus, Applicant submits that claim 16 is allowable.

8. Conclusion

For the foregoing reasons, Applicant submits that claims are allowable. Therefore, Applicant requests favorable reconsideration and allowance of the claims.

Applicant does not acquiesce in any assertion in the office action that is not expressly addressed by these remarks.

Should the Examiner wish to discuss this case with the undersigned, the Examiner is invited to call the undersigned at (312) 913-3350.

Respectfully submitted,

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP

Date: September 26, 2013

By: /Scott M. Miller/
Scott M. Miller
Reg. No. 62,967

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. 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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 11-808-WO-US

Application Number: 13/139,433

Filed: August 15, 2011

For: Frank Muller

Art Unit: 2493

Examiner: Ali Shayanfar

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1400.00
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

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

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 13-2490.

☑ Payment made via EFS-Web.

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.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration number 62,967.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Scott M. Miller/ — Signature

September 26, 2013 — Date

Scott M. Miller — Typed or printed name

312-913-0001 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 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.

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.

Electronic Patent Application Fee Transmittal

Application Number:	13139433
Filing Date:	15-Aug-2011
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Frank Muller
Filer:	Scott Michael Miller/Lisa Panatera
Attorney Docket Number:	11-808-WO-US

Filed as Large Entity

U.S. National Stage under 35 USC 371 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 - 3 months with $0 paid	1253	1	1400	1400

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**1400**

Electronic Acknowledgement Receipt

EFS ID:	16963365
Application Number:	13139433
International Application Number:	
Confirmation Number:	1414
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	Scott Michael Miller
Filer Authorized By:	
Attorney Docket Number:	11-808-WO-US
Receipt Date:	26-SEP-2013
Filing Date:	15-AUG-2011
Time Stamp:	13:04:59
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1400
RAM confirmation Number	18091
Deposit Account	132490
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. 1.492 (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)

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	Amendment Copy Claims/Response to Suggested Claims	11-808-WO-US_response.pdf	67667 df13c9ab98ad859e3afbc9ec62149407b80c1120	no	14
Warnings:					
Information:					
2	Extension of Time	11-808-WO-US_extension.pdf	189065 1d7f858c63ff9e9f65e10ca12530b8bfb6faee15	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30204 41049db23ce05efe73c2d7a80cfc099b35041785	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	286936		

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 (09-11)
Approved for use through 1/31/2014. 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 13/139,433	Filing Date 08/15/2011	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	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 $310 ($155 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	

APPLICATION AS AMENDED – PART II

AMENDMENT **09/26/2013**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 13	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 5	Minus	***5	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					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.

LIE
/RUBY JOHNSON/

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.
13/139,433	08/15/2011	Frank Muller	11-808-WO-US	1414

20306 7590 04/01/2013

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
SHAYANFAR, ALI	

ART UNIT	PAPER NUMBER
2493	

MAIL DATE	DELIVERY MODE
04/01/2013	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)	
	13/139,433	MULLER ET AL.	
	Examiner	Art Unit	
	ALI SHAYANFAR	2493	

-- 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 *13 June 2011*.

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) *1-18* 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) *1-18* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *13 June 2011* 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).

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) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/13/2011, 10/25/2011*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. This is a reply to the application filed on 06/13/2011, in which, claims 1-18 are pending. Claims 1, 9, 12, 14 and 16 are independent. Claims 2-8,10-11, 13, 15, 17-18 are dependent.

Claim Objections

2. The claims 1-2 are objected to because they include reference characters which are not enclosed within parentheses.

Reference characters corresponding to elements recited in the detailed description of the drawings and used in conjunction with the recitation of the same element or group of elements in the claims should be enclosed within parentheses so as to avoid confusion with other numbers or characters which may appear in the claims. See MPEP § 608.01(m).

In claims 1-2, “RES” should have parentheses. Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 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. Claim 1 is rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

Based on Supreme Court precedent[1] and recent Federal Circuit decisions, a §101 process must (1) be tied to another particular apparatus/machine or (2) transform the underlying subject matter (such as an article or materials) to a different state or thing. In addition, the tie to a particular apparatus, for example, cannot be mere extra-solution activity.[2]

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps.

To meet prong (1), the method step should positively recite the other particular apparatus/machine to which it is tied. This may be accomplished by having the claim positively recite the apparatus/machine that accomplishes the method steps. Alternatively or to meet prong (2), the method step should positively recite identifying the material that is being changed to a different state or positively recite the subject matter that is being transformed.

In this particular case, claim fails prong (1) because there exist no "tie" to another particular apparatus/machine to perform the following steps of:

sending a service request for access to a network service….

receiving in response to the service request an authentication request from the network …..

---

[1] See also *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876);

[2] Bilski v. Kappos, 95 USPQ2d 1001 (US 2010));.

identifying the communication channel through which the authentication request was received……..

Therefore, claim does not meet the requirements of the first prong (1).

Additionally, the claim(s) fails prong (2) because the method steps do not transform the underlying subject matter to a different state or thing. While the applicability of other factors for and against subject-matter eligibility has been considered, the weight of the factor(s) described above compels this conclusion. *See Bilski v. Kappos*, 130 S. Ct. 3218, 561 US __ (2010); "Interim Guidance for Determining Subject Matter Eligibility for Process Claims in View of Bilski v. Kappos", 76 Fed. Reg. 43922 (July 27, 2010).

Claims 2, 4-5 are also rejected for being dependent upon rejected claim 1.

In this particular case, claim 2 and 4-5 fails prong (1) because there exist no “tie” to another particular apparatus/machine to perform the following steps of:

determining a service code ……;

calculating the response RES request and the service code…….:

modifying the authentication information on the basis of the identified communications channel…..

generating, preferably using an authentication and key agreement (AKA) of a telecommunication standard…….:. Therefore, claim does not meet the requirements of the first prong (1).

The appropriate correction is required

Claims 9-10 are rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, per se. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. In this case, applicants have claimed a "service interface" in the preamble to the claim without reciting any hardware element in the body of the claim; this implies that Applicants are claiming a system of software, per se, lacking the hardware necessary to realize any of the underlying functionality. Therefore, claim 9-10 are directed to non-statutory subject matter as computer programs, per se.

Claim Rejections - 35 USC § 112

5. The following is a quotation of 35 U.S.C. 112(a):
(a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), first paragraph:
The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 12 and 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

A single means claim, i.e., where a means recitation does not appear in combination with another recited element of means, is subject to an undue breadth

rejection under 35 U.S.C. 112, first paragraph. *In re Hyatt*, 708 F.2d 712, 714-715, 218 USPQ 195, 197 (Fed. Cir. 1983) (A single means claim which covered every conceivable means for achieving the stated purpose was held nonenabling for the scope of the claim because the specification disclosed at most only those means known to the inventor.). When claims depend on a recited property, a fact situation comparable to *Hyatt* is possible, where the claim covers every conceivable structure (means) for achieving the stated property (result) while the specification discloses at most only those known to the inventor. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of 35 U.S.C. 112(b):

(B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

The MPEP interprets claim limitations that contain "if, may, might, can, when and preferably" statement(s), as optional language. As matter of linguistic precision, optional claim elements do not narrow claim limitations, since they can always be omitted.[1] Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation.[2] [3] [4] [5].

Claims 2-5, 9, 11-12 are rejected based on the above explanation.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1, 3-5, 8, 14 and 18 are rejected under 35 U.S.C. 102(b) based as being anticipated by Naslund et al (Publication No. 2006/0288407, hereinafter Naslund) [Applicant's IDS]

As to claim 1Naslund discloses a method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network **(Naslund, Figure, 4, illustrates a user terminal 20, such as a mobile phone or a personal computer, which generally has some form of network communication capabilities 25 such as GSM, Bluetooth)** , the method comprising: sending a service request for access to a network service **(Naslund, discloses communications in GSM, UMTS is triggered as a response to an access request)**; receiving in response to the service request an authentication request from the network **(Naslund, Paragraph [0084] discloses AKA request)**; identifying the communication channel through which the authentication request was received **(Naslund, Paragraph [0084] the terminal (mobile) may be configured to determine whether the AKA request initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces)**; and, sending an authentication response RES to the network, wherein the authentication response depends on the identified communication

channel **(Naslund, Paragraph [0084] and table 1 discloses additional challenge/response depends on communication channel; Paragraph [0110] discloses the modification of the results parameter sent to network)**

As to claim 3 Naslund discloses method according to claim 1, wherein the terminal comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received **(Naslund, Paragraph [0003] discloses many network services are based on storing user credentials (typically a secret key k, and possibly also user identities and pseudonyms) on a tamper-resistant "security device", e.g. a GSM SIM (Subscriber Identity Module), a UMTS SIM or an ISIM (IP Multimedia SIM) card, and letting the network interact with this device through a user terminal in a challenge-response protocol to perform (subscriber) Authentication and Key Agreement (AKA).**

As to claim 4 Naslund discloses method according to claim 1, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising: modifying the authentication information on the basis of the identified communications channel; generating, preferably using an authentication and key agreement (AKA) of a telecommunication standard, an authentication response RES on the basis of the modified authentication

information **(Naslund, Paragraph [0004] In a subscriber database/authentication center, commonly referred to as an AuC in the context of mobile communication systems, an expected response XRES is generated based on knowledge of the secret key and a generated challenge RAND. The AKA protocol may, and typically will, involve an AAA (Authorization, Authentication and Accounting) server, which may or may not be physically co-located with the AuC. The challenge RAND and the expected response XRES are normally transferred to the AAA server. The challenge is sent to the terminal ME (Mobile Equipment), which assisted by the security device computes the response RES. The response is sent back to the AAA server, and if it matches the expected response, the user is authenticated)**

As to claim 5 Naslund discloses a method according to claim 1, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising: generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication standard, an authentication response RES; modifying, preferably using a one-way function, the authentication parameter RES on the basis the identified communications channel **(Naslund, Paragraph [0099] Regardless of the terminal type the SIM is attached to, and the way the SIM is accessed (by Bluetooth, IRDA, in card-reader, etc.) all AKA related processing takes place on the SIM, including the security enhancing steps. The enhanced security processing may involve manipulation of output parameters and/or input parameters of the AKA process, as schematically**

illustrated for a general tamper-resistant security device in FIG. 10.)

As to claim 8 Naslund discloses a method according to claim 1, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface. **(Naslund, Paragraph [0085] Another example of a security policy suitable for implementation in a tamper-resistant security device of the invention is related to the existing proposals for enhancing the security of the 3GPP Gb interface; Paragraph [0084] Paragraph [0084] the terminal (mobile) may be configured to determine whether the AKA request initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces)**

As to claim 14 Naslund in view of ERICSSON discloses a network node for service-based authentication of a terminal to a network, the network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network. **(Naslund, Paragraph [0004] an expected response XRES is generated based on knowledge of the secret key and a generated challenge RAND. The AKA protocol may, and typically will, involve an AAA (Authorization, Authentication and Accounting) server, which may or may not be physically co-**

located with the AuC. The challenge RAND and the expected response XRES are normally transferred to the AAA server. The challenge is sent to the terminal ME (Mobile Equipment), which assisted by the security device computes the response RES. The response is sent back to the AAA server, and if it matches the expected response, the user is authenticated

Claim Rejections - 35 USC § 103

9. 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.

10. Claims 2, 6-7, 9-13, 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naslund et al (Publication No. 2006/0288407, hereinafter Naslund) [Applicant's IDS] in view of (ERICSSON: "How to mitigate the interleaving attack and reduce the trust in the Authenticator (S3-030084)" 3GPP TCG SA WG3 SECURITY, Hereinafter ERICSSON) [Applicant's IDS]

As to claim 2 Naslund discloses all the elements in the claim except determining a service code associated with the identified communication channel; calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information

regarding the identity of the communication channel through which the authentication request was received into the response. ERICSSON discloses determining a service code associated with the identified communication channel; calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information regarding the identity of the communication channel through which the authentication request was received into the response **(ERICSSON, "solution 2" discloses the use of service identifier [service code] in the modified challenge/response to avoid that an attacker re-uses AKA quintets with different service; Page 2, lines7-8, shows authenticator checks that RES=XRES and that the A-Data-MAC is correct, only tha UE that include the correct USIM can calculate both RES and A-data-MAC to alleviate the attack)** It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of ERICSSON by showing determining a service code associated with the identified communication channel; calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information regarding the identity of the communication channel through which the authentication request was received into the response as taught by ERICSSON in order to mitigated the interleaving attack and reduce the trust in authenticator.**(Page2, ERICSSON)**

As to claim 6 Naslund in view of ERICSSON discloses a method according to claim 2, the method further comprising: the terminal sending a service request via a predetermined communications channel to the network; the network generating an expected service code XSC on the basis of the type of communications channel the service request was sent to the network; and determining on the basis of expected service code XSC an expected response XRES. **(ERICSSON, "solution 2", This solution is based on tile idea that the AKA quintet is modified by file HSS in a service dependent way and that file terminal performs file same type of modification. Otherwise the AKA procedure is unchanged. The HSS uses XRES, CK and IK together wifla a service identifier SId to genelxlte derived XRESd, CKd and IKd wifll the help of a pseudo random function: (XRESdllCKdlllKd) = PRF(SIdll XRESIICKIIIK). The derived quintet (Ikd, CKd, RAND, AUTN, XRESd) is sent in message 1. The UE calculates the normal IK, CK and RES and derives IKd, CKd and RESd in the same way that the HSS did. The UE determines the SId to be used on the intended service)**

As to claim 7 Naslund in view of ERICSSON discloses a method according to claim 6, the method further comprising: comparing the expected response XRES with the authentication response RES send by the terminal to the network; and determining the terminal to be in an un-trusted state if RES is not equal to XRES **(ERICSSON, Page 2, lines7-8, shows authenticator checks that RES=XRES and that the A-Data-MAC is correct)**

As to claim 9 Naslund discloses a service interface module for use in a terminal, preferably configured to securely process all authentication information transmitted to and from an identity module in the terminal, the service interface module comprising: a receiver for receiving an authentication signal from the network via one of the communications interfaces of the terminal **(Naslund, Paragraph [0084] discloses AKA request; the invention to maintain the overall security even if a tamper-resistant security device such as a SIM is used in an insecure environment or when reusing the AKA protocol over a less secure interface Paragraph [0004])**; a channel identifier for identifying the communication channel through which the authentication signal was received, **(Naslund, Paragraph [0084] the terminal (mobile) may be configured to determine whether the AKA request initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces)**; a channel interface for establishing a secure communication channel between the module and an identity module of the terminal. **(Naslund, Paragraph [0031], The invention offers the following advantages. [0034] A main merit is that the solution is future proof and easy to administer in a secure way by authenticated downloads. [0035] The solution is in a sense transparent to the device into which the tamper-resistant security device is plugged. In addition, it enables secure remote access directly to the security device, such as a SIM, when the security device is still in the original (mobile) terminal, communicating over e.g. Bluetooth)** Naslund does not disclose preferably by providing a service code

associated with the identified communication channel. ERICSSON disclose preferably by providing a service code associated with the identified communication channel **(ERICSSON, "solution 2" discloses the use of service identifier [service code] in the modified challenge/response to avoid that an attacker re-uses AKA quintets with different service; Page 2, lines7-8, shows authenticator checks that RES=XRES and that the A-Data-MAC is correct, only tha UE that include the correct USIM can calculate both RES and A-data-MAC to alleviate the attack)** It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of ERICSSON by showing preferably by providing a service code associated with the identified communication channel as taught by ERICSSON in order to mitigated the interleaving attack and reduce the trust in authenticator.**(Page2, ERICSSON)**

As to claim 10 Naslund in view of ERICSSON discloses a service interface module according to claim 9, the module further comprising: a modifier for modifying an authentication response of the identity module on the basis of the identified communication channel, or means for transmitting information regarding the identified communications channel to the identity module**(Naslund, Paragraphs [0089] It is of course also important to consider the issue of whether the terminals/handsets remain unaffected by the invention. When the SIM is to be used externally to the terminal/handset, obviously there is no need to change the handset, since it will not even be involved. In the case when the handset is to be used as an**

"authentication token" as discussed above, there is normally a need for modification. However, the mere fact that it should be possible to run GSM AKA commands over IRDA or Bluetooth alone makes modifications necessary (connecting the SIM to Bluetooth/IRDA) or means for modifying the authentication signal received from the network. **(Naslund, Paragraphs [0120] Examples of post-processing of AKA output parameters include: [0121] Combination of a number of generated AKA output parameters (K.sub.c and/or RES) into one or more (possibly longer) modified AKA output parameters (K.sub.c' and/or RES'); [0122] Integrity protection of generated AKA output parameter(s))**

As to claim 11 Naslund in view of ERICSSON discloses an identity module, preferably a smartcard, for establishing a safe communication channel with a service interface module as claimed in claim 9, the identity module comprising: a calculator for calculating a response RES preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA upon receipt of an authentication request; and, optionally, a modifier for modifying the response RES on the basis of a predetermined mathematical function using information on the identified communication channel **(Naslund, Paragraphs [0103-0108] the EAP-SIM protocol that may be generalized and implemented into an AKA cooperating application is authentication of the network over which the user terminal communicates. In normal GSM AKA, the network sends an authentication request together with a RAND, and the SIM simply replies with a response RES. This authentication can be extended by letting the SIM or**

equivalent tamper-resistant security device send a new random value RAND' to the network side in response to the authentication request. The network then calculates a MAC (Message Authentication Code) or similar based on the received RAND' and a session key derived from RAND and the SIM key K, and sends the MAC back to the SIM for verification of the authenticity of the network)

As to claim 12 Naslund in view of ERICSSON discloses a terminal, preferably a mobile device, for accessing network services, the terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal **(Naslund, Paragraphs [0120-0121] discloses an Examples of post-processing of AKA output parameters include: [0121] Combination of a number of generated AKA output parameters (K.sub.c and/or RES) into one or more (possibly longer) modified AKA output parameters (K.sub.c' and/or RES'); [0122] Integrity protection of generated AKA output parameter(s); [0123] Encryption of generated AKA output parameter(s); and [0124] Policy decision and/or enforcement of AKA output parameter(s) based on examination of AKA input parameter(s).**

As to claim 13 Naslund in view of ERICSSON discloses the terminal as recited in claim 12 wherein the terminal is configured to: receive an authentication request from the network; determine a service code associated with the type of communication

channel via which the authentication request was received by the terminal; and send in response to the authentication request an authentication response RES to the network wherein the authentication response depends on the determined service code **(ERICSSON, "solution 2" discloses the use of service identifier [service code] in the modified challenge/response to avoid that an attacker re-uses AKA quintets with different service; Page 2, lines7-8, shows authenticator checks that RES=XRES and that the A-Data-MAC is correct, only that UE that include the correct USIM can calculate both RES and A-data-MAC to alleviate the attack)**

As to claim 15 Naslund in view of ERICSSON discloses a network node as recited in claim 14, wherein the network node is configured to: receive an authentication data request; determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network **(ERICSSON, "solution 2" discloses the use of service identifier [service code] in the modified challenge/response to avoid that an attacker re-uses AKA quintets with different service; Page 2, lines7-8, shows authenticator checks that RES=XRES and that the A-Data-MAC is correct, only that UE that include the correct USIM can calculate both RES and A-data-MAC to alleviate the attack)**; and generate in response to the receipt of the authentication data request an expected response XRES, wherein the expected response depends on the determined expected service code. **(ERICSSON, "solution 2" disclose the HSS uses XRES, CK and IK together wifll a service identifier Sld to genel~lle derived XRESd, CKd and lKd**

with the help of a pseudo random function: (XRESdII(TKdIIIKd) = PRF(SIdII XRESIICKIIIK). The derived quintet (Ikd, CKd, RAND, AUTN, XRESd) is sent in message 1.The UE calculates the normal IK, CK and RES and derives IKd, CKd and RESd in file same way that the HSS did. The UE determines the SId to be used on the intended service.

As to claim 16 Naslund discloses a system for service based authentication to a network, comprising: a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal **(Naslund, Paragraphs [0120-0121] discloses an Examples of post-processing of AKA output parameters include: [0121] Combination of a number of generated AKA output parameters (K.sub.c and/or RES) into one or more (possibly longer) modified AKA output parameters (K.sub.c' and/or RES'); [0122] Integrity protection of generated AKA output parameter(s); [0123] Encryption of generated AKA output parameter(s); and [0124] Policy decision and/or enforcement of AKA output parameter(s) based on examination of AKA input parameter(s))**; Naslund does not discloses a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network. ERICSSON discloses a network

node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network **(ERICSSON, "solution 3" discloses one way to reduce the trust in the Authenticator is to send a modified XRES it: message 1, the Quintet. In order to mitigate pre computation attacks this new XRES denoted XRES' should be calculated by using a Hash function and a nonce value as inputs i.e. XRES'=f2(XRES, nonce).** It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Naslund in view of ERICSSON by showing a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network as taught by ERICSSON in order to mitigated the interleaving attack and reduce the trust in authenticator.**(Page2, ERICSSON)**

As to claim 17 Naslund in view of ERICSSON discloses a system as recited in claim 16, comprising: a terminal configured to receive an authentication request from the network, to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal and to send in response to the authentication request an authentication response RES to the

network wherein the authentication response depends on the determined service code terminal **(Naslund, Paragraphs [0120-0121] discloses an Examples of post-processing of AKA output parameters include: [0121] Combination of a number of generated AKA output parameters (K.sub.c and/or RES) into one or more (possibly longer) modified AKA output parameters (K.sub.c' and/or RES'); [0122] Integrity protection of generated AKA output parameter(s); [0123] Encryption of generated AKA output parameter(s); and [0124] Policy decision and/or enforcement of AKA output parameter(s) based on examination of AKA input parameter(s))**; and a network node configured to receive an authentication data request, determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and to generate in response to the receipt of the authentication data request an expected response XRES, wherein the expected response depends on the determined expected service code **(ERICSSON, "solution 3" discloses one way to reduce the trust in the Authenticator is to send a modified XRES it: message 1, the Quintet. In order to mitigate pre computation attacks this new XRES denoted XRES' should be calculated by using a Hash function and a nonce value as inputs i.e. XRES'=f2(XRES, nonce).**

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US. Publication No. : 2009/0103728 A1 Patel discloses a method and system for secure wireless communications. In particular, the present invention relates to a method of establishing authentication keys at both the network and mobile equipment in order to establish a mutually authenticated communication channel.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALI SHAYANFAR whose telephone number is (571)270-1050. The examiner can normally be reached on Monday through Friday 9:30-6:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Colin Carl can be reached on 571-272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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.

/A. S./
Examiner, Art Unit 2493
3/19/2013

/Carl Colin/

Supervisory Patent Examiner, Art Unit 2493

Notice of References Cited	Application/Control No. 13/139,433	Applicant(s)/Patent Under Reexamination MULLER ET AL.	
	Examiner ALI SHAYANFAR	Art Unit 2493	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2009/0103728	04-2009	Patel, Sarvar	380/247
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	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
	13139433	MULLER ET AL.
	Examiner	**Art Unit**
	ALI SHAYANFAR	2493

✓	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	03/10/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13139433	MULLER ET AL.
	Examiner	Art Unit
	ALI SHAYANFAR	2493

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	3	3/10/2013	AS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search and Assignee search	3/10/2013	AS
EAST Text search: determine, type, channel, connection, authenticate, authentication, policy, XRES, XSC, service request, RES, cryptography	3/10/2013	AS
NPL: Google scholar:Service-Based Authentication to a Network	3/10/2013	AS

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/A.S./ Examiner.Art Unit 2493	

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13139433
Filing Date	2011-08-15
First Named Inventor	Franklin Selgert
Art Unit	2431
Examiner Name	
Attorney Docket Number	11-808-WO-US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.S./

Receipt date: 10/25/2011	Application Number	13139433 13139433 - GAU: 2493
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2011-08-15
	First Named Inventor	Franklin Selgert
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	11-808-WO-US

	1	"3rd Generation Partnership Project; Technical Specification Group SA WG3; A Guide to 3rd Generation Security" (3G TR 33.900 version 1.2.0), (2000-01), pgs. 1-26.	☐
	2	"Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANS), IEEE Std 802.15.1 (2002) 1169 pages.	☐
	3	"Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1:Overview", ETSI EN 300 175-1, V1.9.1, (2005-09) pgs. 1-28.	☐
	4	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 8)', 3GPP TS 33.203 V8.7.0 (2009-09), pgs. 1-114.	☐
	5	"Digital cellular telecommunications system (Phase 2+); Security aspects," (GSM 02.09 version 7.1.1 Release 1998), pgs. 1-11.	☐
	6	"Digital cellular telecommunications system (Phase 2+); Security related network functions," (GSM 03.20 version 7.2.0 Release 1998), pgs. 1-104.	☐
	7	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture," (Release 9), 3GPP TS 33.102 V9.0.0 (2009-09), pgs. 1-70.	☐
	8	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic bootstrapping architecture," (Release 8), 3GPP TS 33.220 V8.7.0 (2009-06), pgs. 1-75.	☐
	9	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)," (Release 8), 3GPP TS 33.222 V8.0.0 (2008-06), pgs. 1-23.	☐
	10	"3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function," (Release 8), 3GPP TS 33.223 V8.5.0 (2009-09), pgs. 1-23.	☐
	11	"3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Generic Access Network (GAN); Stage 2," (Release 8), 3GPP TS 43.318 V8.4.0 (2009-02), pgs. 1-127.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.S./

Receipt date: 10/25/2011	Application Number	13139433 13139433 - GAU: 2493
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2011-08-15
	First Named Inventor	Franklin Selgert
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	11-808-WO-US

If you wish to add additional non-patent literature document citation information please click the Add button			Add
EXAMINER SIGNATURE			
Examiner Signature	/Ali Shayanfar/	Date Considered	03/10/2013

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.S./

Receipt date: 10/25/2011	Application Number	13139433	13139433 - GAU: 2493
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2011-08-15	
	First Named Inventor	Franklin Selgert	
	Art Unit	2431	
	Examiner Name		
	Attorney Docket Number	11-808-WO-US	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the 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. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Scott M. Miller/	Date (YYYY-MM-DD)	2011-10-25
Name/Print	Scott M. Miller	Registration Number	62,967

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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.S./

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 the Freedom of Information Act requires disclosure of these record s.

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 inspections 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.S./

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. 1414

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/139,433	08/15/2011	726	2493	11-808-WO-US

APPLICANTS
Frank Muller, Delft, NETHERLANDS;
Franklin Selgert, Berkel en Rodenrijs, NETHERLANDS;

**** CONTINUING DATA ***************************
This application is a 371 of PCT/EP09/67201 12/15/2009

**** FOREIGN APPLICATIONS ***************************
EUROPEAN PATENT OFFICE (EPO) 08021705.2 12/15/2008

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
08/18/2011

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/ALI SHAYANFAR/ Examiner's Signature	☐ Initials	NETHERLANDS	5	18	5

ADDRESS

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606
UNITED STATES

TITLE

Service-Based Authentication to a Network

FILING FEE RECEIVED		
1550	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

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	2011-06-13
First Named Inventor	Franklin Selgert
Art Unit	TBA
Examiner Name	TBA
Attorney Docket Number	11-808-WO-US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060288407		2006-12-21	Naslund et al.	
	2	20050228992		2005-10-13	Mizikovsky	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.S./

Receipt date: 06/13/2011	Application Number	13139433 - GAU: 2493
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2011-06-13
	First Named Inventor	Franklin Selgert
	Art Unit	TBA
	Examiner Name	TBA
	Attorney Docket Number	11-808-WO-US

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report and Written Opinion, International Application No. PCT/EP2009/067201 dated February 26, 2010.	☐
	2	ERICSSON, "How to Mitigate the Interleaving Attack and Reduce the Trust in the Authenticator", 3GPP TSG SA WG3 Security, February 2003, pp. 1-3.	☐
	3	European Seach Report, European Patent Application No. 08021705.2 dated June 5, 2009.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Ali Shayanfar/	Date Considered	03/10/2013

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.S./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	183	AKA and RES and XRES and (authentication) and challenge	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/20 15:30
L4	86	AKA and RES and XRES and (authentication) and challenge and channel	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/20 15:30
S1	174	((FRANK) near2 (MULLER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/10 22:49
S2	25	((FRANKLIN) near2 (SELGERT)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/10 22:49
S3	30	(determin$) near3 (type) near4 (channel connection) with (authentic$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:49
S4	9	(determin$3 detect$4 based) near3 (type) near4 (channel connection) with (authentic$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:50
S5	103	(determin$ detect$4 based) near3 (type) near4 (channel connection) with (authentic$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:51
S6	61	(determin$) near3 (type) near4 (channel connection) with (policy)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:51
S7	61	(determin$) near3 (type) near4 (channel connection) with (policy)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:52
S8	22	(determin$) near3 policy near3 (type) near4 (channel connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:52
S9	147	(determin$) near3 (policy authentic$) near3 (type) near4 (session channel connection)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:53
S10	6	(determin$) near3 (policy authentic$) near3 (type) near4 (session channel connection) near2 network$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:53
S11	3825	726/3.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 22:55

Samsung Ex. 1002, Page 146 of 341

S12	28	Service-Based same Authentication same Network	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/03/10 23:52
S13	606	(NEDERLANDSE ORGANISATIE VOOR TOEGEPAST).as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/10 23:55
S14	1	S12 and S13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/10 23:55
S15	2	"20060288407"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/10 23:57
S16	2	"2005228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 01:59
S17	2	"2006288407"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:01
S18	2	"20060288407"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:02
S19	2	"2005228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:02
S20	3	"20050228992"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 02:03
S21	2	"20070283425"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2013/03/11 23:31

EAST Search History (Interference)

< This search history is empty>

3/ 20/ 2013 3:54:38 PM
C:\ Users\ ashayanfar\ Documents\ EAST\ Workspaces\ 13139433.wsp

Samsung Ex. 1002, Page 147 of 341

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
13/139,433	08/15/2011	Frank Muller	11-808-WO-US

CONFIRMATION NO. 1414

20306
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

PUBLICATION NOTICE

OC000000051243036

Title: Service-Based Authentication to a Network

Publication No.US-2011-0296494-A1
Publication Date:12/01/2011

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13139433
Filing Date	2011-08-15
First Named Inventor	Franklin Selgert
Art Unit	2431
Examiner Name	
Attorney Docket Number	11-808-WO-US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13139433
	Filing Date	2011-08-15
	First Named Inventor	Franklin Selgert
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	11-808-WO-US

	1	"3rd Generation Partnership Project; Technical Specification Group SA WG3; A Guide to 3rd Generation Security" (3G TR 33.900 version 1.2.0), (2000-01), pgs. 1-26.	☐
	2	"Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANS), IEEE Std 802.15.1 (2002) 1169 pages.	☐
	3	"Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1:Overview", ETSI EN 300 175-1, V1.9.1, (2005-09) pgs. 1-28.	☐
	4	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 8)', 3GPP TS 33.203 V8.7.0 (2009-09), pgs. 1-114.	☐
	5	"Digital cellular telecommunications system (Phase 2+); Security aspects," (GSM 02.09 version 7.1.1 Release 1998), pgs. 1-11.	☐
	6	"Digital cellular telecommunications system (Phase 2+); Security related network functions," (GSM 03.20 version 7.2.0 Release 1998), pgs. 1-104.	☐
	7	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture," (Release 9), 3GPP TS 33.102 V9.0.0 (2009-09), pgs. 1-70.	☐
	8	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic bootstrapping architecture," (Release 8), 3GPP TS 33.220 V8.7.0 (2009-06), pgs. 1-75.	☐
	9	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)," (Release 8), 3GPP TS 33.222 V8.0.0 (2008-06), pgs. 1-23.	☐
	10	"3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function," (Release 8), 3GPP TS 33.223 V8.5.0 (2009-09), pgs. 1-23.	☐
	11	"3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Generic Access Network (GAN); Stage 2," (Release 8), 3GPP TS 43.318 V8.4.0 (2009-02), pgs. 1-127.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13139433
	Filing Date	2011-08-15
	First Named Inventor	Franklin Selgert
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	11-808-WO-US

If you wish to add additional non-patent literature document citation information please click the Add button Add			
EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13139433
	Filing Date	2011-08-15
	First Named Inventor	Franklin Selgert
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	11-808-WO-US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the 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. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Scott M. Miller/	Date (YYYY-MM-DD)	2011-10-25
Name/Print	Scott M. Miller	Registration Number	62,967

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 1 hour 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.**

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 the Freedom of Information Act requires disclosure of these record s.

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 inspections 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.

Electronic Acknowledgement Receipt

EFS ID:	11250799
Application Number:	13139433
International Application Number:	
Confirmation Number:	1414
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	Scott Michael Miller
Filer Authorized By:	
Attorney Docket Number:	11-808-WO-US
Receipt Date:	25-OCT-2011
Filing Date:	15-AUG-2011
Time Stamp:	11:18:13
Application Type:	U.S. National Stage under 35 USC 371

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	Non Patent Literature	33900.pdf	202792 fc308158d063b785f93e786dbf01fc22fd5945ed	no	26
Warnings:					
Information:					

2	Non Patent Literature	802151_Part1.pdf	24387764 cc4cf704b6abb2bd209ed8bed623427fc37c5825	no	100
Warnings:					
Information:					
3	Non Patent Literature	802151_Part2.pdf	22191264 ea567639756af494343bf4f784234d905824a59a	no	95
Warnings:					
Information:					
4	Non Patent Literature	802151_Part3.pdf	18845316 2949ae191565dad31fee754104045248ac097cc0	no	100
Warnings:					
Information:					
5	Non Patent Literature	802151_Part4.pdf	19083033 915e1200852a47aefdc31b553f048433dd3c2e87	no	95
Warnings:					
Information:					
6	Non Patent Literature	802151_Part5.pdf	18700676 c3484f6bdace651fade0ab8b80d7e27e05984ebf	no	100
Warnings:					
Information:					
7	Non Patent Literature	802151_Part6.pdf	9006593 8004e684a1c6896d4f8841fcf5ae2485e9b0c444	no	95
Warnings:					
Information:					
8	Non Patent Literature	802151_Part7.pdf	17524400 0387e046fe0f75fe791c7d7f31883b4d83bb51c6	no	195
Warnings:					
Information:					
9	Non Patent Literature	802151_Part8.pdf	17280224 e36c466cc25cb83735a73d3ec14fc6e1768ecfc4	no	195
Warnings:					
Information:					
10	Non Patent Literature	802151_Part9.pdf	24281747 a35aef5c175e6a43ece9daa194cacae65ab53f9f	no	194
Warnings:					
Information:					

11	Non Patent Literature	300175.pdf	3196766 cc45c76100abf1c54e9cfd34ae0f1bde5ec865bf	no	28
Warnings:					
Information:					
12	Non Patent Literature	33203.pdf	8179999 669da1b4ab6f2d3c952baead5c328f0e889d7bcd	no	114
Warnings:					
Information:					
13	Non Patent Literature	GSM0209.pdf	1030103 f0f80f5cf0bffe98bef700d2c32e05ece78779a5	no	11
Warnings:					
Information:					
14	Non Patent Literature	GSM0320.pdf	8273305 b6dfdd68dd291735076fdc9442a97caa02858d0e	no	104
Warnings:					
Information:					
15	Non Patent Literature	33102.pdf	530804 ce36bb7dc206c94c249628674e53055558df6e69	no	70
Warnings:					
Information:					
16	Non Patent Literature	33220.pdf	599874 9512dd99f9f76d255f8a58a400f4c4f1b5caf65a	no	75
Warnings:					
Information:					
17	Non Patent Literature	33222.pdf	279694 bdd3b948b2322c86656494010a835019b618c623	no	22
Warnings:					
Information:					
18	Non Patent Literature	33223.pdf	306117 c75784600c6e4a91b9ca48bd468e309606aac489	no	23
Warnings:					
Information:					
19	Non Patent Literature	43318.pdf	1024924 2e9282dfd5230761fe653b3b2a92233ffa3a8703	no	127
Warnings:					
Information:					

20	Information Disclosure Statement (IDS) Form (SB08)	11_808_WO_US_IDS.pdf	613130 ea34cb89efd6c980890c14dd10f5fac146cb457d	no	5

Warnings:

Information:

A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.

Total Files Size (in bytes):	195538525

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/139,433	08/15/2011		1550	11-808-WO-US	18	5

CONFIRMATION NO. 1414

20306
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

FILING RECEIPT

OC000000049416699

DOCKETED

AUG 23 2011

DUE

BY SSO

Date Mailed: 08/19/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Frank Muller, Delft, NETHERLANDS;
Franklin Selgert, Berkel en Rodenrijs, NETHERLANDS;

Assignment For Published Patent Application

KONINKLIJKE KPN N.V., The Hague, NL /Nederlandse Organisatie Voor Toegepast-Natuurwetenschappelijk Onderzoek TNO, Delft, NL

Power of Attorney: The patent practitioners associated with Customer Number 20306

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP09/67201 12/15/2009

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
EUROPEAN PATENT OFFICE (EPO) 08021705.2 12/15/2008

If Required, Foreign Filing License Granted: 08/18/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/139,433**

Projected Publication Date: 12/01/2011

Non-Publication Request: No

Early Publication Request: No

Title

Service-Based Authentication to a Network

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier

license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
(Case No. 11-808-WO-US)

In the Application of:	)	
	)	
Frank Muller et al.	)	
	)	**Examiner: TBD**
Serial No.: 13/139,433	)	
	)	**Group Art Unit: TBD**
Filing Date: August 15, 2011	)	
	)	**Confirmation No.: 1414**
For: Service-Based Authentication to a Network	)	

REQUEST FOR CORRECTED FILING RECEIPT

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

Attention: Application Processing Division
Customer Correction Branch

Dear Sir:

Attached is a copy of the official filing receipt received from the PTO in the above-referenced application which issuance of a corrected filing receipt is respectfully requested.

There is an error with respect to the following data, which is incorrectly entered. The Assignment for Published Patent Application is missing one of the Assignees. The Assignment information should read as follows:

Assignment for Published Patent Application:

KONINKLIJKE KPN N.V., The Hague, NL
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO, Delft, NL

The Application Data Sheet submitted on June 13, 2011 correctly reflects this information.

Respectfully submitted,

Date: September 8, 2011

By: /Scott M. Miller/
Scott M. Miller
Registration No. 62,967

McDonnell Boehnen Hulbert & Berghoff LLP
300 South Wacker Drive, 32nd Floor
Chicago, IL 60606
(312)913-0001

Electronic Acknowledgement Receipt

EFS ID:	10896839
Application Number:	13139433
International Application Number:	
Confirmation Number:	1414
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Frank Muller
Customer Number:	20306
Filer:	Scott Michael Miller
Filer Authorized By:	
Attorney Docket Number:	11-808-WO-US
Receipt Date:	08-SEP-2011
Filing Date:	15-AUG-2011
Time Stamp:	12:59:38
Application Type:	U.S. National Stage under 35 USC 371

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 Corrected Filing Receipt	11_808_WO_US_Filing_Receipt.pdf	347810 6dec6b884f00b654f615079d66b012da325e8f13	no	3

Warnings:	
Information:	

2	Request for Corrected Filing Receipt	11_808_WO_US_Request_Correct_Filing_Receipt.pdf	20718 861dad49e56031bcab4ce06ff8174cf61c377a25	no	1

Warnings:	
Information:	
Total Files Size (in bytes):	368528

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/139,433	08/15/2011		1550	11-808-WO-US	18	5

CONFIRMATION NO. 1414

CORRECTED FILING RECEIPT

20306
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

OC000000049744029

Date Mailed: 09/08/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Frank Muller, Delft, NETHERLANDS;
Franklin Selgert, Berkel en Rodenrijs, NETHERLANDS;

Assignment For Published Patent Application

KONINKLIJKE KPN N.V., The Hague, NL
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO, Delft, NETHERLANDS

Power of Attorney: The patent practitioners associated with Customer Number 20306

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP09/67201 12/15/2009

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
EUROPEAN PATENT OFFICE (EPO) 08021705.2 12/15/2008

If Required, Foreign Filing License Granted: 08/18/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/139,433**

Projected Publication Date: 12/01/2011

Non-Publication Request: No

Early Publication Request: No

Title

Service-Based Authentication to a Network

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier

license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

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

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
13/139,433	Frank Muller	11-808-WO-US

20306
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

INTERNATIONAL APPLICATION NO.	
PCT/EP09/67201	
I.A. FILING DATE	PRIORITY DATE
12/15/2009	12/15/2008

CONFIRMATION NO. 1414
371 ACCEPTANCE LETTER

OC000000049416700

Date Mailed: 08/19/2011

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office in its capacity as a Designated / Elected Office (37 CFR 1.495), has determined that the above identified international application has met the requirements of 35 U.S.C. 371, and is ACCEPTED for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

08/15/2011	08/15/2011
DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS	DATE OF COMPLETION OF ALL 35 U.S.C. 371 REQUIREMENTS

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1), (c)(2) and (c)(4) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE.** *The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363).* Once the Filing Receipt has been received, send all correspondence to the Group Art Unit designated thereon.

The following items have been received:

- Copy of the International Application filed on 06/13/2011
- Copy of the International Search Report filed on 06/13/2011
- Preliminary Amendments filed on 06/13/2011
- Information Disclosure Statements filed on 06/13/2011
- Oath or Declaration filed on 08/15/2011
- U.S. Basic National Fees filed on 06/13/2011
- Priority Documents filed on 06/13/2011

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

VALERIE D KINARD

Telephone: (703) 756-1432

FORM PCT/DO/EO/903 (371 Acceptance Notice)

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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/139,433	08/15/2011		1550	11-808-WO-US	18	5

CONFIRMATION NO. 1414

20306
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

FILING RECEIPT

OC000000049416699

Date Mailed: 08/19/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Frank Muller, Delft, NETHERLANDS;
Franklin Selgert, Berkel en Rodenrijs, NETHERLANDS;

Assignment For Published Patent Application

KONINKLIJKE KPN N.V., The Hague, NL

Power of Attorney: The patent practitioners associated with Customer Number 20306

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP09/67201 12/15/2009

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
EUROPEAN PATENT OFFICE (EPO) 08021705.2 12/15/2008

If Required, Foreign Filing License Granted: 08/18/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/139,433**

Projected Publication Date: 12/01/2011

Non-Publication Request: No

Early Publication Request: No

Title

Service-Based Authentication to a Network

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier

license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/139,433

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	330
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	430
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	220
TOTAL CLAIMS (37 CFR 1.16(i))	18 minus 20 =	*			OR	x 52 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	5 minus 3 =	* 2				x 220 =	440
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $270 ($135 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).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1420

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	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	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	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 found in the appropriate box in column 1.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)
(Case No. 11-808-WO-US)

In re Application of:	)	
	)	
Franklin Selgert et al.	)	
	)	**Examiner: TBA**
Serial No.: 13/139,433	)	
Int'l Appln. No.: PCT/EP2009/067201	)	**Art Unit: TBA**
	)	
Int'l. Filing Date: December 15, 2009	)	**Conf. No. 1414**
	)	
For: Service-Based Authentication to a Network	)	

RESPONSE TO NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 MAILED ON JUNE 29, 2011

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notification of Missing Requirements Under 35 U.S.C. 371 mailed June 29, 2011, Applicants submit herewith an executed Declaration and Power of Attorney in compliance with 37 CFR § 1.497(a) and (b). Please charge the surcharge of **$130.00** and any deficiency in the amount due, or credit any overpayment, to Deposit Account No. **13-2490**. Applicants believe that no further fees are due. If the Examiner believes otherwise, the Commissioner is authorized to deduct any fee from the Deposit Account No. 13-2490.

Applicants submit that the response to the Notice is complete. Prompt consideration and entry of this response and attachments are respectfully requested.

Respectfully submitted,

Date: August 15, 2011

/Scott M. Miller/
Scott M. Miller
Registration No. 62,967

McDonnell Boehnen Hulbert & Berghoff LLP
300 South Wacker Drive, 32nd Floor
Chicago, IL 60606
(312) 913-0001

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

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

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Service-based authentication to a network

the specification of which is attached hereto unless the following space is checked:

X was filed on 13 June 2011 as United States Application Serial Number 13/139,433

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

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).

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

Prior Foreign Application(s):

	Number	Country	Day/Month/Year Filed
1.	08021705.2	EP	15/12/2008
2.	PCT/EP2009/067201	WO	15/12/2009

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below:

	Application Number	Filing Date
1.		

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

I hereby appoint the practitioners associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and I direct that all correspondence be addressed to that Customer Number.

Customer Number: **020306**

Principal attorney or agent: Bradley Hulbert
Telephone number: 312-913-0001

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 Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

The undersigned hereby authorize and request the attorneys of record in said application to insert in this declaration and power of attorney the filing date and serial number of said application when officially known, if the specification is not attached hereto.

Full name of first inventor: Frank Muller

Inventor's signature: _____ Date: 12 juli 2011
Residence: Hopstraat 59, 2611 TB Delft, The Netherlands
Citizenship: The Netherlands
Post Office Address: Hopstraat 59, 2611 TB Delft, The Netherlands

Full name of second inventor: Franklin Selgert

Inventor's signature: _____ Date: _____
Residence: Penninglaan 30, 2651 BL Berkel en Rodenrijs
Citizenship: The Netherlands
Post Office Address: Penninglaan 30, 2651 BL Berkel en Rodenrijs

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

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

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Service-based authentication to a network

the specification of which is attached hereto unless the following space is checked:

X was filed on 13 June 2011 as United States Application Serial Number 13/139,433

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

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).

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

Prior Foreign Application(s):

	Number	Country	Day/Month/Year Filed
1.	08021705.2	EP	15/12/2008
2.	PCT/EP2009/067201	WO	15/12/2009

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below:

	Application Number	Filing Date
1.		

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

I hereby appoint the practitioners associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and I direct that all correspondence be addressed to that Customer Number.

Customer Number: **020306**

Principal attorney or agent: Bradley Hulbert
Telephone number: 312-913-0001

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 Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

The undersigned hereby authorize and request the attorneys of record in said application to insert in this declaration and power of attorney the filing date and serial number of said application when officially known, if the specification is not attached hereto.

Full name of first inventor: Frank Muller

Inventor's signature: _____ Date: _____
Residence: Hopstraat 59, 2611 TB Delft, The Netherlands
Citizenship: The Netherlands
Post Office Address: Hopstraat 59, 2611 TB Delft, The Netherlands

Full name of second inventor: Franklin Selgert

Inventor's signature: _____ Date: 05-07-2011
Residence: Penninglaan 30, 2651 BL Berkel en Rodenrijs
Citizenship: The Netherlands
Post Office Address: Penninglaan 30, 2651 BL Berkel en Rodenrijs

Electronic Patent Application Fee Transmittal

Application Number:	13139433
Filing Date:	
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Franklin Selgert
Filer:	Scott Michael Miller/Holly Mueller
Attorney Docket Number:	11-808-WO-US

Filed as Large Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Oath/decl > 30 months from priority date	1617	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**130**

Electronic Acknowledgement Receipt

EFS ID:	10731737
Application Number:	13139433
International Application Number:	
Confirmation Number:	1414
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Franklin Selgert
Customer Number:	20306
Filer:	Scott Michael Miller
Filer Authorized By:	
Attorney Docket Number:	11-808-WO-US
Receipt Date:	15-AUG-2011
Filing Date:	
Time Stamp:	01:10:12
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$130
RAM confirmation Number	7169
Deposit Account	132490
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. 1.492 (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)

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	Applicant Response to Pre-Exam Formalities Notice	11_808_WO_US_Response.pdf	92398 3e27d9abd3b66212addbd7bbc3263114532efa40	no	1
Warnings:					
Information:					
2	Oath or Declaration filed	11_808_WO_US_Declaration.pdf	101809 4ab897a1b1aadc74e39a0605d8e6a0b5ae7fb401	no	4
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	29900 ad6f24787bec71e0fb56348a6ba839b744d7b3b3	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	224107		

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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/139,433

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	330
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	430
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	220
TOTAL CLAIMS (37 CFR 1.16(i))	18 minus 20 =	*			OR	x 52 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	5 minus 3 =	* 2				x 220 =	440
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $270 ($135 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).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1420

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT A	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	

		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	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 found in the appropriate box in column 1.

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

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
13/139,433	Franklin Selgert	11-808-WO-US

20306
MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

INTERNATIONAL APPLICATION NO.	
PCT/EP09/67201	
I.A. FILING DATE	PRIORITY DATE
12/15/2009	12/15/2008

CONFIRMATION NO. 1414
371 FORMALITIES LETTER



Date Mailed: 06/29/2011

NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as a Designated Office (37 CFR 1.494):

- Priority Document
- Copy of the International Application filed on 06/13/2011
- Copy of the International Search Report filed on 06/13/2011
- Preliminary Amendments filed on 06/13/2011
- Information Disclosure Statements filed on 06/13/2011
- U.S. Basic National Fees filed on 06/13/2011
- Priority Documents filed on 06/13/2011

The applicant needs to satisfy supplemental fees problems indicated below.

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Oath or declaration of the inventors, in compliance with 37 CFR 1.497(a) and (b), identifying the application by the International application number and international filing date.
- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.492(h) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fees required for this application is $**130** for a Large Entity:
- $**130** Surcharge.

ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTHS FROM THE DATE OF THIS NOTICE OR BY 32 MONTHS FROM THE PRIORITY DATE FOR THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

VALERIE D KINARD

Telephone: (703) 756-1432

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

Substitute for Form PTO-1360
(For use with Form PTO/SB/06)

Application Number	Filing Date
13139433	

Applicant(s) Franklin Selgert

* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT	
	Indep	Depend	Indep	Depend	Indep	Depend
1	1		1			
2		1		1		
3		2		1		
4		(1)		1		
5		(1)		1		
6		(1)		1		
7		(1)		1		
8		(1)		1		
9	1		1			
10		1		1		
11		2		1		
12	1		1			
13		1		1		
14	1		1			
15		1		1		
16	1		1			
17		1		1		
18		(1)		1		
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
Total Indep	5		5		0	
Total Depend	15	↵	13	↵	0	↵
Total Claims	20		18		0	

	*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
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						

PTO-1390 (Rev. 09-08)
Approved for use through 3/31/2010. OMB 0651-0021
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 LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 11-808-WO-US

U.S. APPLICATION NO. (If known, see 37 CFR 1.5):

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP2009/067201	December 15, 2009	December 15, 2008

TITLE OF INVENTION: Service-Based Authentication to a Network

APPLICANT(S) FOR DO/EO/US: SELGERT, Franklin; MULLER, Frank

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☑ This is a **FIRST** submission of items concerning a submission under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a submission under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☑ The US has been elected (Article 31).
5. ☑ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☑ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☑ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☑ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☑ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☑ A preliminary amendment.
14. ☑ An Application Data Sheet under 37 CFR 1.76.
15. ☐ A substitute specification.
16. ☐ A power of attorney and/or change of address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821- 1.825.
18. ☑ A second copy of the published International Application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. 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 15 minutes to complete, including gathering information, preparing, and submitting the completed 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: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
	PCT/EP2009/067201	11-808-WO-US

20. Other items or information:

International Search Report (PCT/ISA/210);
International Written Opinion (PCT/ISA/237);
PCT/IB/304 Form

The following fees have been submitted	CALCULATIONS	PTO USE ONLY
21. ☑ Basic national fee (37 CFR 1.492(a))..... **$330**	$ 330	
22. ☑ Examination fee (37 CFR 1.492(c)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)..... **$0** All other situations..... **$220**	$ 220	
23. ☑ Search fee (37 CFR 1.492(b)) If the written opinion of the ISA/US or the International preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)..... **$0** Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority..... **$100** International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB..... **$430** All other situations..... **$540**	$ 430	
TOTAL OF 21, 22 and 23 =	980.00	

☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)).
The fee is **$270** for each additional 50 sheets of paper or fraction thereof.

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round **up** to a whole number)	RATE	
- 100 =	/50 =		x $**270**	$

Surcharge of **$130.00** for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	- 20 =		x $ **52**	$	
Independent claims	- 3 =	2	x **$220**	$ 440.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$390**	$	
			TOTAL OF ABOVE CALCULATIONS =	$ 1420.00	
☐ Applicant claims small entity status. See 37 CFR 1.27. Fees above are reduced by ½.					
			SUBTOTAL =	$ 1420.00	
Processing fee of **$130.00** for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)). +				$	
			TOTAL NATIONAL FEE =	$ 1420.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$	
			TOTAL FEES ENCLOSED =	$ 1420.00	
			Amount to be refunded:	$	
			Amount to be charged	$	

a. ☐ A check in the amount of $ _____ to cover the above fees is enclosed.

b. ☑ Please charge my Deposit Account No. 13-2490 in the amount of $ 1420.00 to cover the above fees.

c. ☑ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 13-2490.

d. ☐ Fees are to be charged to a credit card. **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. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended paying fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

SEND ALL CORRESPONDENCE TO:

Customer No. 20306
McDonnell Boehnen Hulbert & Berghoff LLP
300 South Wacker Drive
Chicago, Illinois 60606
(312) 913-0001 (Telephone)
(312) 913-0002 (Facsimile)
Date: June 13, 2011

/Scott M. Miller/
SIGNATURE

Scott M. Miller
NAME

62,967
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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	2011-06-13
First Named Inventor	Franklin Selgert
Art Unit	TBA
Examiner Name	TBA
Attorney Docket Number	11-808-WO-US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060288407		2006-12-21	Naslund et al.	
	2	20050228992		2005-10-13	Mizikovsky	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2011-06-13
	First Named Inventor	Franklin Selgert
	Art Unit	TBA
	Examiner Name	TBA
	Attorney Docket Number	11-808-WO-US

Examiner Initials*	Cite No	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, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report and Written Opinion, International Application No. PCT/EP2009/067201 dated February 26, 2010.	☐
	2	ERICSSON, "How to Mitigate the Interleaving Attack and Reduce the Trust in the Authenticator", 3GPP TSG SA WG3 Security, February 2003, pp. 1-3.	☐
	3	European Seach Report, European Patent Application No. 08021705.2 dated June 5, 2009.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2011-06-13
	First Named Inventor	Franklin Selgert
	Art Unit	TBA
	Examiner Name	TBA
	Attorney Docket Number	11-808-WO-US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the 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. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Scott M. Miller/	Date (YYYY-MM-DD)	2011-06-13
Name/Print	Scott M. Miller	Registration Number	62967

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 1 hour 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.**

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 the Freedom of Information Act requires disclosure of these record s.

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 inspections 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.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
KONINKLIJKE KPN N.V.
Attn. Wuyts, Koenraad
P.O. Box 95321
NL-2509 CH The Hague
PAYS-BAS

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 403332WO	Date of mailing *(day/month/year)* 26/02/2010
International application No. PCT/EP2009/067201	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
Applicant KONINKLIJKE KPN N.V.	International filing date *(day/month/year)* 15/12/2009

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority 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	Authorized officer Anita Rothenbücher

Form PCT/ISA/220 (July 2009) *(See notes on accompanying sheet)*

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims,description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Annex B).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, International Phase, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet or sheets containing a complete set of claims in replacement of all the claims previously filed must be submitted.

Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively in Arabic numerals (Section 205(a)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide.*

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims,description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Annex B).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, International Phase, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet or sheets containing a complete set of claims in replacement of all the claims previously filed must be submitted.

Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively in Arabic numerals (Section 205(a)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
403332WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/EP2009/067201	15/12/2009	15/12/2008
Applicant		
KONINKLIJKE KPN N.V.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/067201

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06

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)
H04W H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/288407 A1 (NASLUND MATS [SE] ET AL) 21 December 2006 (2006-12-21)	1,3-5, 8-12,14, 16,18
Y	paragraph [0003] paragraphs [0006] - [0009] paragraph [0014] paragraph [0024] paragraphs [0035], [0036] paragraphs [0056] - [0064] paragraphs [0074] - [0077] paragraphs [0084] - [0087]; table 1 paragraphs [0099] - [0102] paragraphs [0108] - [0113]	2,6-7, 13,15,17

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family 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
19 February 2010	26/02/2010

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, Fax: (+31-70) 340-3016	Ruiz Sanchez, J

1

Form PCT/ISA/210 (second sheet) (April 2005)

Samsung Ex. 1002, Page 197 of 341

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/228992 A1 (MIZIKOVSKY SEMYON B [US]) 13 October 2005 (2005-10-13) paragraph [0017]; figure 1 paragraphs [0024] - [0031]; figure 3	1,3-5, 8-12,14, 16,18
Y	ERICSSON: "How to mitigate the Interleaving attack and reduce the trust in the Authenticator (S3-030084)" 3GPP TSG SA WG3 SECURITY, February 2003 (2003-02), XP050243902 the whole document	2,6-7, 13,15,17

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/067201

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006288407 A1	21-12-2006	NONE	
US 2005228992 A1	13-10-2005	NONE	

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2009/067201	15.12.2009	15.12.2008

International Patent Classification (IPC) or both national classification and IPC
INV. H04W12/06

Applicant
KONINKLIJKE KPN N.V.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office
P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tel. +31 70 340 - 2040
Fax: +31 70 340 - 3016

Date of completion of this opinion

see form PCT/ISA/210

Authorized Officer

Ruiz Sanchez, J

Telephone No. +31 70 340-4717

Form PCT/ISA/237 (Cover Sheet) (April 2005)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material:

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing:

      ☐ contained in the international application as filed.

      ☐ filed together with the international application in electronic form.

      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2, 6-7, 13, 15, 17
	No:	Claims	1, 3-5, 8-12, 14, 16, 18
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-18
Industrial applicability (IA)	Yes:	Claims	1-18
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1 US 2006/288407 A1 (NASLUND MATS [SE] ET AL) 21 December 2006

D2 US 2005/228992 A1 (MIZIKOVSKY SEMYON B [US]) 13 October 2005

D3 ERICSSON: "How to mitigate the Interleaving attack and reduce the trust in the Authenticator (S3-030084)" 3GPP TSG SA WG3 SECURITY, February 2003

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1, 9, 11, 12, 14, 16, 18 is not new.

2.1 Document D1 discloses (the references in parentheses applying to this document) a method for service - based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting - up a communication channel with the network (figure 4, the mobile terminal comprises several communication units: e.g GSM, UMTS, Bluetooth...), the method comprising the steps of:

- sending a service request for access to a network service (this step is implicitly disclosed, since authentication in the services disclosed in D1, e.g. GSM, UMTS... is triggered as a response to an access request);

- receiving in response to the service request an authentication request from the network (paragraph [0084]: "AKA request");

- identifying the communication channel through which the authentication request was received (paragraph [0084], first sentence: "...the terminal (mobile) may be configured to determine whether the AKA request initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces"); and,

- sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel (paragraph [0084] and table 1: additional processing of the challenge/ response depends on the communication channel; paragraph [0110] shows the modification of the result parameter sent to the network).

2.2 The same reasoning applies mutatis mutandis to independent claims 9, 11, 12, 14, 16, 18. The subject-matter of claims 9, 11, 12, 14, 16, 18 is therefore not new.

2.3 For the sake of completeness, it is noticed that document D2 discloses dual terminals using the same identification module for authenticating the network access via two different network interfaces (paragraph [0025]) wherein the response of the terminal to the authentication request depends on the communication channel used. According to D2 the authentication information received from the network is treated differently depending on the access interface used: in the case of IS-2000, the standard challenge/response with CAVE is performed (paragraph [0025], third sentence), whereas in the case of HRPD, the authentication information is modified by the terminal before passing it to the identity module (paragraph [0027]) and the response received from the identity module is modified (paragraphs [0029] and [0030]). The corresponding modifications of the information received by the HLR/AuC are performed by the AAA in the network side (paragraph [0030]). Therefore, the subject-matter of claims 1, 9, 11, 12, 14, 16, 18 is also considered not new over disclosure D2.

2.4 The attention of the applicant is also drawn to the fact that commonly used USIM/SIM/ISIM modules fall into the scope of claim 11, since the modification of the standard response on the basis of a predetermined function and the identified communication channel are defined as optional.

3 Claims 2-8, 10, 13, 15, 17 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT with respect to novelty and/or inventive step:

3.1 The additional features of claims 3-5, 8, 10 are known from D1 (see point 2.1 above and the corresponding passages cited on the search report, in particular paragraphs [0024], [0036], [0056] and [0087]).

3.2 The additional features of claims 2, 6, 7, 13, 15, 17 are rendered obvious by the combination of documents D1 (see paragraphs [0020] and [0108] to [0111]) and D3 (see page 2, "solution 2", which teaches the use of a service identifier in the modified challenge/response to avoid that an attacker re-uses AKA quintets with a different service).

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information	For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.
Amending claims under Art. 19 PCT	Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.
Filing a demand for international preliminary examination	In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT). If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).
Filing informal comments	After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.
End of the international phase	At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).
Relevant PCT Rules and more information	Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

BNSDOCID: <XS_____ 200704010CK | >

Bitte beachten Sie, dass angeführte Nichtpatentliteratur (wie z. B. wissenschaftliche oder technische Dokumente) je nach geltendem Recht dem Urheberrechtsschutz und/oder anderen Schutzarten für schriftliche Werke unterliegen könnte. Die Vervielfältigung urheberrechtlich geschützter Texte, ihre Verwendung in anderen elektronischen oder gedruckten Publikationen und ihre Weitergabe an Dritte ist ohne ausdrückliche Zustimmung des Rechtsinhabers nicht gestattet.

Veuillez noter que les ouvrages de la littérature non-brevets qui sont cités, par exemple les documents scientifiques ou techniques, etc., peuvent être protégés par des droits d'auteur et/ou toute autre protection des écrits prévue par les législations applicables. Les textes ainsi protégés ne peuvent être reproduits ni utilisés dans d'autres publications électroniques ou imprimées, ni rediffusés sans l'autorisation expresse du titulaire du droit d'auteur.

Please be aware that cited works of non-patent literature such as scientific or technical documents or the like may be subject to copyright protection and/or any other protection of written works as appropriate based on applicable laws. Copyrighted texts may not be copied or used in other electronic or printed publications or re-distributed without the express permission of the copyright holder.

XS CPRTENFRDE

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	11-808-WO-US
	Application Number	
Title of Invention	Service-Based Authentication to a Network	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Franklin		Selgert	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Berkel en Rodenrijs	Country Of Residence[i]	NL
Citizenship under 37 CFR 1.41(b)[i]	NL		

Mailing Address of Applicant:

Address 1	Penningslaan 30		
Address 2			
City	Berkel en Rodenrijs	State/Province	
Postal Code	NL-2651 BL	Country[i]	NL

Applicant 2 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Frank		Muller	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Delft	Country Of Residence[i]	NL
Citizenship under 37 CFR 1.41(b)[i]	NL		

Mailing Address of Applicant:

Address 1	Hopstraat 39		
Address 2			
City	Delft	State/Province	
Postal Code	NL-2611 TB	Country[i]	NL

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	11-808-WO-US
	Application Number	
Title of Invention	Service-Based Authentication to a Network	

Customer Number	20306		
Email Address	docketing@mbhb.com	Add Email	Remove Email

Application Information:

Title of the Invention	Service-Based Authentication to a Network		
Attorney Docket Number	11-808-WO-US	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	5	**Suggested Figure for Publication (if any)**	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and 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 international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	20306		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	a 371 of international	PCT/EP2009/067201	2009-12-15

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	11-808-WO-US
	Application Number	
Title of Invention	Service-Based Authentication to a Network	

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
08021705.2	EP	2008-12-15	(•) Yes ( ) No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Remove

Assignee 1

If the Assignee is an Organization check here. [X]

Organization Name	Koninklijke KPN N.V.		
Mailing Address Information:			
Address 1	Maanplein 55		
Address 2			
City	The Hague	**State/Province**	
Country [i]	NL	Postal Code	NL-2516 CK
Phone Number		Fax Number	
Email Address			

Remove

Assignee 2

If the Assignee is an Organization check here. [X]

Organization Name	Nederlandse Organisatie Voor Toegepast-Natuurwetenschappelijk Onderzoek TNO		
Mailing Address Information:			
Address 1	Schoemakerstraat 97		
Address 2			
City	Delft	**State/Province**	
Country [i]	NL	Postal Code	NL-2628 VK
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Scott M. Miller/	Date (YYYY-MM-DD)	2011-06-13

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	11-808-WO-US
	Application Number	
Title of Invention	Service-Based Authentication to a Network	

First Name	Scott M.	Last Name	Miller	Registration Number	62967

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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.**

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 the Freedom of Information Act requires disclosure of these records.

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 inspections 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.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 June 2010 (24.06.2010)

PCT

(10) International Publication Number
WO 2010/069962 A1

(51) International Patent Classification:
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/EP2009/067201

(22) International Filing Date:
15 December 2009 (15.12.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08021705.2 15 December 2008 (15.12.2008) EP

(71) Applicants *(for all designated States except US)*: **KONINKLIJKE KPN N.V.** [NL/NL]; Maanplein 55, NL-2516 CK The Hague (NL). **NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO** [NL/NL]; Schoemakerstraat 97, NL-2628 VK Delft (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SELGERT, Franklin** [NL/NL]; Penningslaan 30, NL-2651 BL Berkel en Rodenrijs (NL). **MULLER, Frank** [NL/NL]; Hopstraat 39, NL-2611 TB Delft (NL).

(74) Agent: **WUYTS, Koenraad**; P.O. Box 95321, NL-2509 CH The Hague (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: SERVICE-BASED AUTHENTICATION TO A NETWORK

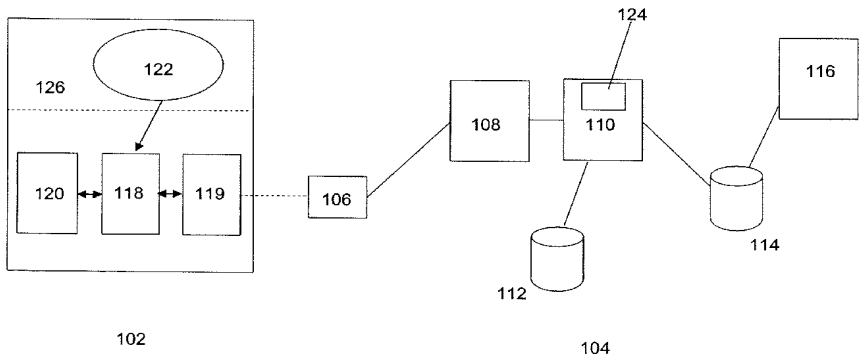


Figure 1

(57) **Abstract**: A method and a system for service-based authentication of a terminal to a network is described, wherein the terminal comprises a number of communications interfaces, each communications interface allowing the terminal to set-up a predetermined communication channel with the network. The method comprises the steps of: sending a service request for access to a network service; receiving in response to the service request an authentication request from the network; identifying the communication channel through which the authentication request was received; and, sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

WO 2010/069962 A1

Service-based authentication to a network.

Field of the invention

The invention relates to a service-based authentication to a network and, in particular, though not exclusively, to a method and a system for a service-based authentication of a terminal to a network and a service interface module for use in such system.

Background of the invention

The new generation mobile devices, such as smart phones, provide more and more enhanced computational functionalities via open network connections. Such mobile devices are e.g. capable of receiving e-mail, share software with one another through short-range connections, downloading and executing software from the Internet, making automated calls and act under remote control. Hence, similar to a personal computer, mobile devices and in particular the software components involved in the setting up of a connection between the mobile device to the network, are vulnerable to attacks of malicious code (malware). Typically malware attempts to make misuse of mobile device or to simply disrupt legitimate use of a mobile device.

Typically, malware makes use of security flaws in the authentication procedure which provides a subscriber access to a network. For example the GSM authentication and key agreement (AKA) only authenticates the mobile device to the network, but not the other way around. The GSM AKA is therefore vulnerable to so-called false base station attacks wherein an attacker pretends to be a valid base station. In the UMTS AKA part of these threats are mitigated by using a mutual authentication wherein the mobile device has to authenticate itself to the Visitor Location Register (VLR) and the VLR has to authenticate itself to the mobile device. An overview of the security threats in the GSM AKA and the way a

number of these threats are counteracted by the UMTS AKA are described in ETSI TS 33.900.

From TS 33.900 it follows that the UMTS AKA is still vulnerable to security attacks. For example, the UMTS AKA is vulnerable to the so-called man-in-the-middle attacks, wherein a mobile device of an attacker may use authentication information from the (U)SIM of the victim in order to obtain access to the network. Such a man-in-the-middle attack allows network access as if the connection was set up by the victim. As the network cannot distinguish between a legal situation and such attack the malware allows to set up calls on the expenses of the victim thereby causing substantial damage.

Summary of the invention

It is an object of the invention to reduce or eliminate at least one of the drawbacks known in the prior art and to provide in a first aspect of the invention a method for service-based authentication of a terminal to a network. The terminal comprises one or more communications interfaces for allowing the terminal to setting-up a communication channel with the network. The method comprises the steps of: sending a service request for access to a network service; receiving in response to the service request an authentication request from the network; identifying the communication channel through which the authentication request was received; and, sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

The method allows the network to determine through which communication channel authentication information is transmitted to the network. Determination of the communication channel can be easily achieved by identifying the communication interface through which the authentication request is received. Such service-based authentication method effectively prevents misuse of authentication information, e.g. a man-in-the-middle attack wherein an attacker uses

authentication information from the (U)SIM of the victim in order to obtain access to the network.

Furthermore, the method is compatible with all or at least most existing and proposed AKA's. It only requires determination of the communication channel through which the request was received and secure insertion of information regarding the communication channel into the response.

In one embodiment the method further comprises the steps of: determining a service code associated with the identified communication channel; calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information regarding the identity of the communication channel through which the authentication request was received into the response.

The information regarding the communication channel through which the authentication information is transmitted to the network is securely inserted in the response of the identity module of the terminal. Hence, it is not possible or at least very difficult for malware to detect and/or modify the service channel information.

In another embodiment the terminal used in the method comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.

By using a service interface module as a trusted hardware module in the terminal, a very safe and reliable method is achieved for sending the information regarding the identity of the communication channel to the network. Preferably, the service interface module is configured to receive all incoming authentication signals from the network. Hence, all authentication request will be routed via the service interface module to the identity module of the terminal.

In yet another embodiment the authentication request comprises authentication information, preferably a random

challenge RAND and the method further comprises the steps of: modifying the authentication information on the basis of the identified communications channel; generating, preferably using an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES on the basis of the modified authentication information.

In one embodiment the authentication request comprises authentication information, preferably a random challenge RAND and the method further comprises the steps of: generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES; modifying, preferably using a one-way function, the authentication parameter RES on the basis the identified communications channel.

This embodiment allows simple and safe implementation of the method by using a service interface module which securely communicates with the identity module. Identification of the communication channel and secure insertion of the information regarding the identified communication channel may take place in the service interface module so that no modifications of the identity module are required. This implementation is thus compatible with existing identity modules.

In another embodiment the method further comprises the steps of: the terminal sending a service request via a predetermined communications channel to the network; the network generating an expected service code XSC on the basis of the type of communications channel the service request was sent to the network; determining on the basis of expected service code XSC an expected response XRES.

In one embodiment the method further comprises the steps of: comparing the expected response XRES with the authentication response RES send by the terminal to the network; and, determining the terminal to be in an un-trusted state if RES is not equal to XRES.

Hence, the method only requires a simple modification in the existing network in the sense that it requires a network node which is configured to identify the communication channel through which the service request is received by the network and to extract the information regarding the communication channel encrypted in the terminal response.

In one embodiment the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

In a further aspect the invention relates to a service interface module for use in a terminal, preferably configured to securely process all authentication information transmitted to and from an identity module in the terminal, wherein the service interface module comprises: a receiver for receiving an authentication signal from the network via one of the communications interfaces of the terminal; a channel identifier for identifying the communication channel through which the authentication signal was received, preferably by providing a service code associated with the identified communication channel; an interface for establishing a secure communication channel between the module and an identity module of the terminal.

All functionality required in the terminal for implementation of the method can be simply located in one trusted hardware module which securely communicates with the identity module.

In one embodiment the service interface module further comprises a modifier for modifying an authentication response of the identity module on the basis of the identified communication channel, or sender for transmitting information regarding the identified communications channel to the identity module, or modifier for modifying the authentication request received from the network.

In another aspect the invention relates to an identity module, preferably a smartcard, for establishing a safe communication channel with a service interface module as described above. The safe communication channel may for

example consist of a link protected with cryptography or a direct hardware link between the service interface module and the identity module that cannot be interfered with by an attacker. The identity module comprises: a calculator for calculating a response RES - preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA - upon receipt of an authentication request; and, optionally, a modifier for modifying the response RES on the basis of a predetermined mathematical function using information on the identified communication channel.

In yet another aspect the invention relates to a terminal, preferably a mobile device, for accessing network services, wherein the terminal is configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal.

In one embodiment the terminal comprises a service interface module according as described and, optionally, an identity module as described above.

In a further aspect the invention relates to a network node for service-based authentication of a terminal to a network, wherein the network node is configured to generate in response to the receipt of an authentication data request a modified expected response XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

In one embodiment the network node comprises: a receiver for receiving a service request from a terminal; a generator for generating an expected service code XSC on the basis of the type of communication channel the service request was sent to the network; a generator for generating an expected response XRES or a receiver for receiving from another network node an expected response XRES, preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA; and, a modifier the expected response XRES on the basis of a predetermined mathematical function, preferably a one-way

function, using the expected service code XSC as an input parameter.

In one embodiment the network node further comprises: a receiver for receiving a response RES from a terminal; a comparator for comparing the response RES with the modified expected response XRES'.

In yet a further aspect the invention relates to a system for service based authentication to a network, comprising: a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal; and, a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

The invention also relates to a computer program product comprising software code portions configured for, when run in the memory of a terminal, preferable a mobile device, executing the method steps as described above.

The invention will be further illustrated with reference to the attached drawings, which schematically will show embodiments according to the invention. It will be understood that the invention is not in any way restricted to these specific embodiments.

Brief description of the drawings

Fig. 1 depicts a schematic representation of a system according to one embodiment of the invention.

Fig. 2 illustrates a schematic flow diagram of the GSM authentication procedure and the UMTS authentication procedure.

Fig. 3 depicts the service interface module according to one embodiment of the invention.

Fig. 4 depicts a flow diagram according to one embodiment of the invention.

Fig. 5 illustrates prevention of a fraudulous authentication procedure by using the invention.

Detailed description

Fig. 1 illustrates a schematic representation of a communications system **100** according to one embodiment of the invention. The system comprises a terminal **102** connected to a communications network **104**. In one embodiment the network may be a 2G-type (e.g. GSM) mobile network comprising a base transceiver station (BTS) **106** serving as an access node. The BSC is connected via a base station controller (BSC) **108** to a mobile switching center (MSC) **110** of e.g. a visiting network (VN). The MSC is linked to a visited location register (VLR) **112**, which is a database that stores user related data and performs security functions. The MSC is further linked to a home location register (HLR) **114** which is located in the home network (HN) where the user of the terminal **102** has a subscription with the network operator. The HLR **114** stores user related data, e.g. subscription related data, and co-operates with the MSC/VLR **110** to keep track of the location of the terminal. The HLR is connected to an authentication centre (AuC) **116**. The authentication centre (AuC) comprises (amongst others) algorithms for the calculation of authentication parameters used in the authentication procedure. For each subscriber the AuC stores a secret authentication key K which is also stored in an associated identity module, e.g. a (U)SIM card or the like, located in the terminal.

Alternatively, the network in Fig. **1** may also depict a 3G-type (e.g. UMTS) mobile network comprising 3G network elements. In that case, the network may comprise a radio base station (Node-B) **106** connected via a Radio Network Controller (RNC) **108** to a Serving GPRS Support Node (SGSN) **110**. The SGSN is further connected to a VLR **112** and an AuC/HLR **114,116** in a similar way as in the 2G-type network as described above.

In a further embodiment the communications network **104** may comprise IMS-based network elements in the form of a set of Call/Session Control Functions (CSCF) such as a Proxy-CSCF (P-CSCF), an Interrogating-CSCF (I-CSCF), a Serving-CSCF (S-CSCF) and a Home Subscriber Server (HSS). In yet further embodiments the communications network may comprise 3GPP LTE or 3GPP SAE network elements.

The terminal **102** may be a personal computer or a mobile device such as a smart phone, a personal digital assistant (PDA), a laptop or any other mobile communications device capable of providing services over one or more networks. The terminal comprises a service interface (SI) module **118**, an operating system (OS) **126** and an identity module **120**.

The SI module **118** acts as a central access point to wired and wireless network services and comprises for that purpose a number of service interfaces. For example, for wireless services, it includes an interface to an RF module, e.g. a 2G or 3G radio card, comprising an RF receiver connecting to one more antennas. **Fig. 1** depicts an exemplary implementation wherein a radio card module **119** provides radio contact with the base station **106**. The RF interface of the radio card is capable of receiving and/or transmitting RF signals in accordance with various wireless technologies using licensed frequency bands (e.g. TDMA for GSM services or W-CDMA for UMTS services). The radio card must have a secure interface to the SI module. Beside the interface to the RF module the SI module may comprise a number of interfaces to other wireless interface modules, e.g. wireless interface modules using non-licensed frequency bands such as the IEEE 802.11 interface for WLAN services, the IEEE 802.15.1 interface for Bluetooth services, an DECT interface as described in ETS 300 175, etc.

The SI module may also comprise interfaces to one or more wired interface modules, e.g. an Ethernet interface allowing the SI module to be connected to the network using a wired Ethernet communication channel. An access and configuration (AC) manager in the SI module manages the set-up

of a communication channel to an access node of a network or - in case of a short-range connection such as Bluetooth - to another terminal. It determines the correct parameter for operation under a specific wired or wireless technology and/or protocol associated with the networks services requested by the terminal. Further, the SI module is configured to securely include information regarding the used interface in the data sent to a Service Identification Unit (SIU) **124** in the network. The interaction between the SI module **118** and the SIU **124** is explained hereunder in more detail.

The Operating System (OS) of the terminal comprises a kernel which manages the resources of the mobile device e.g. the Central Processing Unit (CPU), memory for storing program instructions and data and Input/Output (I/O) devices such as the radio module. Further, the OS comprises Application Programming Interfaces (APIs) through which application programs **122** may access services offered by the OS. The OS may comprise APIs for setting up wired or wireless connections via one of the interfaces modules.

The identity module **120**, which is typically removable, may be a UICC (Universal Integrated Circuit Card) for use in mobile devices suitable for 2G-type network services (GSM) or 3G-type network services, (UMTS). To that end, the UICC may comprise a Subscriber Identity Module (SIM) application comprising SIM functions and/or a UMTS Subscriber Identity Module (USIM) application comprising USIM functions. It is to be understood that the identity module is not limited to SIM and/or USIM applications. In further embodiments, the identity module may be an IP Multimedia Sub-system SIM (ISIM) for authenticating and accessing IMS-based services according to a predetermined IMS-based AKA as e.g. described in ETSI technical specification TS 33.203 or an extensible authentication protocol (EAP) based SIM for authentication and accessing a network according to a predetermined EAP-based AKA as described for instance in RFC4187.

The identity module may comprise a processor, one or more memory components e.g. ROM, RAM and/or EEPROM and I/O circuitry. For authentication purposes the UICC comprises a

secret service-subscriber authentication key K and one or more algorithms for calculating a response comprising one or more authentication parameters upon the reception of a random challenge.

Fig. 2(a) illustrates a schematic flow diagram of the standard GSM authentication procedure which may be used by the SIM module in the identity module. In the GSM standard the MSC initiates, in response to a service request of a network service originating from the terminal, a request for authentication data to the AuC/HLR (step **202**). A random number generator at the AuC/HLR generates a random value RAND that is input to the GSM A3/A8 algorithms which generate an expected response XRES and a cipher key K_C. The triplet {RAND, XRES, K_C} is returned to the MSC (step **204**) that subsequently forwards the RAND value to the SIM card of the terminal (step **206**). Corresponding calculations are performed by the terminal, typically by the integrity module, which returns a calculated response RES back to the MSC (step **208**). By comparison of the RES with the XRES the MSC can authenticate the terminal to the network.

In the standard UMTS authentication procedure similar steps as the GSM procedure are performed. However, in order to improve the security additional parameters and a set of eight functions f0-f5,f1*,f2* are used. **Fig. 2(b)** illustrates a schematic flow diagram of the UMTS authentication procedure, which may be used with a USIM application in the identity module. In response to a request for authentication data from the SGSN/VLR (step **210**), the AuC/HRL generates a random number RAND (using function f0) and a fresh sequence number SQN. The AuC/HRL provides the secret authentication key K (which is both stored in the AuC and the USIM but never directly exchanged) and an operator specific Authentication Management Field AMF. These four parameters are fed into the five symmetric encryption functions f1-f5, resulting in five new parameters: the Message Authentication Code (MAC), the Expected Response (XRES), the Ciphering Key (CK), the Integrity Key (IK) and the Anonymity Key (AK). The sequence number SQN is separately encrypted into SQN^1.

The AuC/HLR returns these parameters in an authentication vector (AV) {AUTN,RAND,XRES,CK,IK} to the SGSN/VLR (step **212**) wherein the Authentication token AUTN is a triplet {SQN^1,AMF,MAC}. Thereafter, the SGSN/VLR forwards an Authentication and Ciphering request comprising RAND and AUTN to the mobile device (step **214**). Using RAND and AUTN the USIM calculates - amongst others - a response RES, which is sent back to the SGSN (step **216**) and compared with the XRES as received from the AuC/HLR.

The keys for ciphering and integrity checking have a limited lifetime to prevent attempts to break the cipher or integrity protection by brute force long duration monitoring attacks. Upon expiry, a new set of ciphering and integrity keys are generated with a re-authentication between the terminal and the network. This re-authentication process is regularly repeated.

The GSM AKA is described in detail in ETSI standards GSM 02.09 and GSM 03.20 and the UMTS AKA described in detail in ETSI technical specification TS 33.102, which are hereby incorporated by reference.

Fig. 3 depicts an SI module according to a preferred embodiment of the invention The SI module **300** is located in a terminal **322** and comprises a number of interfaces **302a-302e**, which are connected, preferably through one or more secure communication channels , to associated interface modules **320a-320e**. The interface modules are located in the terminal and used for setting up a network connection with the network **316**. The SI module is configured to generate a service code (SC) identifying the specific service interface used to set up a wired or a wireless communication channel. To that end, the AC manager **304** in the SI module may use a look-up table **306** comprising the different types of service interfaces supported by the mobile terminal and the associated service codes. The AC manager may be implemented in the form of a processor and one or more memory modules comprising e.g. the configuration data of the look-up table.

The hardware of the terminal is preferably configured in such a way that all incoming authentication requests for a

network service received by one of the interfaces **302a-302e** will be centrally routed via the SI module to the UICC connected to the SI module. Such hardware architecture ensures that all incoming authentication requests are identified with respect to the communication channel the request was received by the terminal. Further, the SI module is configured to provide a secure communication channel **308** with the UICC **310** connected to the SI module. Hence, preferably, the SI module is implemented in the form of one or more trusted hardware components.

If, for example, the terminal **322** receives a network signal, e.g. a 3G signal, via a 3G RF interface module **320c** and the 3G interface **302c** of the SI module, the signal is translated into a digital signal in accordance with the technical specifications of the wireless air interface. Thereafter the digital signal comprising the authentication request is transmitted via the SI module to the UICC **310**. Further, the AC manager **304** identifies the service code associated with the 3G RF interface **302c** using a look-up table **306**. The service code is used by the SI module to provide the network with information regarding the origin of the authentication request.

The UICC processes the authentication request according to an AKA of a telecommunications standard, e.g. a GSM AKA or a UMTS AKA as described in relation with **Fig. 2** and then returns a response RES back to the SI module. Thereafter, the SI module uses a predetermined mathematical algorithm f stored in a secure memory **312** of the SI module in order to securely include the information embodied in the service code into the response RES received from the UICC. Preferably, the mathematical algorithm f is a so-called one-way function which is easy to compute but impossible or very hard to invert. A suitable one-way function may be a secure hash operation with the SC. Inserting the service code into the response allows the SI module to inform the network **316** about the communication channel (Bluetooth **314a**, WLAN **314b**, 3G **314c**, Ethernet **314d**, etc.) through which the authentication request

was received from the network in a way which is not, or at least very difficult, to modify by malware.

In order for the network to extract the channel information, the network, preferably the SGSN/VLR or an equivalent network node such as the MCS/VLR, comprises an Service Identification Unit (SIU). The SIU comprises a function f which is identical to the function f used by the SI module. Further, the SIU is configured to determine through what type of communication channel a service request is received.

The advantage of the architecture of the SI module as depicted in **Fig. 3** is that the specifications of the (U)SIM do not require changes. The implementation is simple and only requires the installation of a SI module in the terminal and a SIU in the network. Moreover, the architecture is backwards compatible with conventional equipment, i.e. terminals and network nodes (e.g. SGSN/VLR or MCS/VLR) which do not comprise a SI mode or a SIU.

A more detailed explanation on the functioning of the SIU will be given in relation to **Fig. 4**.

Fig. 4 depicts a process flow **400** between a UMTS network and a terminal comprising a USIM and an SI module as described in relation with **Fig. 1** and **3**. The process is started by a terminal application requesting a UMTS service from the network. The request triggers the RF interface module to set-up up a wireless UMTS communication channel between the terminal and an access node of the requested UMTS network. Thereafter, a service request is transmitted via the wireless communication channel to the SGSN/VLR (step **402**).

Then the SIU in the SGSN/VLR determines through which service interface (UMTS, GSM, WiFi, Bluethooth, etc.) contact was established with the terminal. On the basis of the identified service interface information an expected service code XSC is determined (step **404**). The SIU may determine XSC by retrieving the service code associated with the identified service interface (in this case a UMTS service) from a look-up table - substantially identical to the one used by the SI

module in the terminal - stored in a secure memory of the SI module.

In response to the service request, the SGSN/VLR sends an authentication data request to the AuC/HLR of the network (step **406**). The AuC/HLR generates a UMTS authentication vector AV, which is sent back to the SGSN/VLR (step **408**). Subsequently RAND and AUTN are sent in an Authentication and Ciphering request via the wireless communication channel to the terminal (step **410**). When the RF interface module of the terminal receives the radio signal comprising the request, the signal is converted to a digital signal. The AC manager identifies the service code associated with the interface used by the SI module to communicate with the RF module (step **412**). Thereafter, the digital signal comprising the RAND and AUTN is forwarded to the USIM (step **414**), which calculates the response RES using e.g. the f1-f5 algorithms of the UMTS AKA. Then the USIM sends the response RES back to the SI module (step **416**).

Using the SC and the one-way function f, the SI determines a modified response RES'=f(RES,SC) (step **418**), hence securely inserting information about the communication channel through which the request was received. This way, the response RES' becomes specific for the service it is meant for. The response RES' is subsequently transmitted back via RF interface to the SGSN/VLR in the network (step **420**) for comparison with an expected response XRES' (step **422**). The expected response XRES' may be determined by the SIU using the one-way function f with the expected response XRES determined on the basis of the UMTS AKA and the SC as the input parameters: XRES'=f(XRES,SC).

Thereafter a comparison between the terminal response RES' and the expected response XRES' is made. If RES' is equal to XRES' then this provides an indication for the network that the terminal received an authentication request via the communication channel that was expected by the network. In that case access to the network is granted.

If RES' is not equal to XRES' then an indication to the network is provided that the terminal received an

authentication request via a communication channel different from the communication channel expected by the network. This may provide the network with an indication that the terminal may be corrupted by malware.

It is noted that the invention is not limited to the embodiment as described in relation with **Fig. 3** and **4**. In a further embodiment the UICC (instead of the SI module) comprises the one-way function f for securely inserting the service code information into the response.

After the AC manager has selected the correct SC, the code is inserted into the digital signal comprising the request and send to the identity module for further processing (e.g. authentication and/or computation of the decryption key). Hence, in this variant the digital signal sent by the SI module to the identity module comprises information via which service interface (and hence via which communications channel) the signal was received. Further variants for sending the service code to the identity module may include, e.g. sending the service code to the identity module in a separate signal.

In one embodiment the (U)SIM may modify the authentication information in the authentication request, e.g. a random challenge RAND, on the basis of the service code SC and subsequently calculate a response RES on the basis of an authentication and key agreement (AKA) of a telecommunications standard. For example, in the case of a GSM service the SIM may perform the steps: RAND'=f(RAND,SC) and RES'=A3(RAND',K_C). In another variant, the SIM first calculates the response RES on the basis of the RAND and then modifies RES on the basis of SC: RES=A3(RAND,K_C) and RES'=f(RES,SC). In the case of an UMTS service, the f1-f5 algorithms of the UMTS AKA are used instead of the A3 algorithm of the GSM AKA.

Depending on the specific scheme implemented in the USIM, the SIU which comprises the mathematical function f used by the USIM in the terminal, may determine RAND'=f(RAND, XSC) and send this value to the AuC/HLR for determining the expected response XRES' on the basis the UMTS AKA using RAND' as one of the input parameters. Alternatively, the AuC/HRL may first determine XRES on the basis the UMTS AKA using RAND as

one of the input parameters and then send this value to the SIU for determining the expected response XRES'=f(XRES,XSC).

Fig. 5 represents a simplified schematic illustrating how a fraudulous authentication procedure may be prevented using the invention. In this scheme a first terminal **502** of an attacker remotely connects to an infected second terminal **504** of a victim and subsequently requests and uses authentication information from the (U)SIM **506** of the victim to obtain access to the network **510**.

The malware in the second terminal **504** allows the terminal of an attacker **502** to make a first communication channel **512**, e.g. a Bluetooth connection, with the infected terminal of the victim. Other types of connections such as a WiFi connection or a wired connection, such as an Ethernet connection, may also be possible. After connecting to the victim, the attacker starts an authentication procedure to the network by sending a service request via a second communication channel **514** to the AuC/HRL. In response, the attacker will receive an authentication request comprising - amongst others - RAND and AUTN. Instead of responding to the request, the attacker forwards the request to the victim using the Bluetooth connection to the (U)SIM of the victim .

A conventional (U)SIM cannot distinguish between requests originating from different communication channels (e.g. UMTS, GSM, WiFi, Bluetooth, etc.). In that case, the (U)SIM responds to the request by calculating a correct response RES, which is subsequently send via the Bluetooth connection (i.e. the communication connection where the request came from) to the network. The attacker may use this RES to authenticate itself successfully to the network. Using this mechanism the attacker is capable of correctly answering each subsequent Authentication and Ciphering Request from the network.

If however the network **510** and the infected terminal **504** in **Fig.5** are configured as a communications system according to the invention as described in relation with **Fig.1**, the SI module **508** is able to make a distinction between requests originating from different sources. In that case, the

network **510** will determine an expected service code XSC on the basis of the request of the attacker. As the attacker requested a UMTS service via second communication channel **514**, the network will set the XSC to the service code corresponding to a UMTS service. Similarly, the SI module **508** of the infected terminal will modify the RES using the service code corresponding to a Bluetooth communications channel **512**. This modified RES' is sent via the Bluetooth connection to the network, which will then determine that the XRES' calculated by the network on the basis of XSC does not match RES' because the communication channel used to send a request for a UMTS service to the network is different from the communication channel through which the terminal received the authentication request. In that case, the network may take appropriate action.

In one embodiment, the network may calculate the expected response values (XRES'', XRES''', etc.) for each service code available in the look-up table located in a service node of the network. If a XRES' value associated with a particular service code matches RES' then the source of the request received by the terminal may be determined.

This information may be used by the network to take appropriate action. It may e.g. provide no or limited access to the network or place the mobile device in a separate isolation or quarantine network in order to provide remediation services to the mobile device of the subscriber. If the response RES' is neither equal to XRES' nor to the other expected responses then the authentication procedure has failed.

It is to be understood that the invention may also be used with the IMS AKA (3GPP TS 33.203), in Generic Bootstrapping (GBA) applications (see 3GPP TS 33.220, 33.222, 33.223) or with the EAP AKA and/or EAP SIM in WLAN interworking applications. It can also be used in generic access solutions to the mobile network (see 3GPP TS 43.318).

Further, it is to be understood that any feature described in relation to any one embodiment may be used alone, or in combination with other features described, and may also

be used in combination with one or more features of any other of the embodiments, or any combination of any other of the embodiments. Furthermore, equivalents and modifications not described above may also be employed without departing from the scope of the invention, which is defined in the accompanying claims.

CLAIMS

1. Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising the steps of:
- sending a service request for access to a network service;
- receiving in response to the service request an authentication request from the network;
- identifying the communication channel through which the authentication request was received; and,
- sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

2. Method according to claim 1, the method further comprising the steps of:
- determining a service code associated with the identified communication channel;
- calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information regarding the identity of the communication channel through which the authentication request was received into the response.

3. Method according to claims 1 or 2, wherein the terminal comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.

4. Method according to any of claims 1 to 3, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising the steps of:

- modifying the authentication information on the basis of the identified communications channel;
- generating, preferably using an authentication and key agreement (AKA) of a telecommunication standard, an authentication response RES on the basis of the modified authentication information.

5. Method according to any of claims 1 to 3, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising the steps of:

- generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication standard, an authentication response RES;
- modifying, preferably using a one-way function, the authentication parameter RES on the basis the identified communications channel.

6. Method according to any of claims 2-5, the method further comprising the steps of:

- the terminal sending a service request via a predetermined communications channel to the network;
- the network generating an expected service code XSC on the basis of the type of communications channel the service request was sent to the network;
- determining on the basis of expected service code XSC an expected response XRES.

7. Method according to claim 6, the method further comprising the steps of:

- comparing the expected response XRES with the authentication response RES send by the terminal to the network; and,

- determining the terminal to be in an un-trusted state if RES is not equal to XRES.

8. Method according to any of claims 1-7, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

9. Service interface module for use in a terminal, preferably configured to securely process all authentication information transmitted to and from an identity module in the terminal, the service interface module comprising:

- a receiver for receiving an authentication signal from the network via one of the communications interfaces of the terminal;
- a channel identifier for identifying the communication channel through which the authentication signal was received, preferably by providing a service code associated with the identified communication channel;
- a channel interface for establishing a secure communication channel between the module and an identity module of the terminal.

10. Service interface module according to claim 9, the module further comprising:

- a modifier for modifying an authentication response of the identity module on the basis of the identified communication channel, or means for transmitting information regarding the identified communications channel to the identity module, or means for modifying the authentication signal received from the network.

11. An identity module, preferably a smartcard, for establishing a safe communication channel with a service interface module as claimed in claims 9 or 10, the identity module comprising: a calculator for calculating a response RES - preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA

- upon receipt of an authentication request; and, optionally, a modifier for modifying the response RES on the basis of a predetermined mathematical function using information on the identified communication channel.

12. A terminal, preferably a mobile device, for accessing network services, the terminal being configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal.

13. The terminal as recited in claim 12 wherein the terminal is configured to:

- receive an authentication request from the network;
- determine a service code associated with the type of communication channel via which the authentication request was received by the terminal and;
- send in response to the authentication request an authentication response RES to the network wherein the authentication response depends on the determined service code.

14. A network node for service-based authentication of a terminal to a network, the network node being configured to generate in response to the receipt of an authentication data request a modified expected response XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

15. A network node as recited in claim 14 wherein the network node is configured to:

- receive an authentication data request;
- determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and;

- generate in response to the receipt of the authentication data request an expected response XRES, wherein the expected response depends on the determined expected service code.

16. A system for service based authentication to a network, comprising:

- a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal;
- a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

17. A system as recited in claim 16, comprising:

- a terminal configured to receive an authentication request from the network, to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal and to send in response to the authentication request an authentication response RES to the network wherein the authentication response depends on the determined service code and;
- a network node configured to receive an authentication data request, determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and to generate in response to the receipt of the authentication data request an expected response XRES, wherein the expected response depends on the determined expected service code.

18. A computer program product comprising software code portions configured for, when run in the memory of a terminal, preferable a mobile device, executing the method steps according to any of claims 1-5.

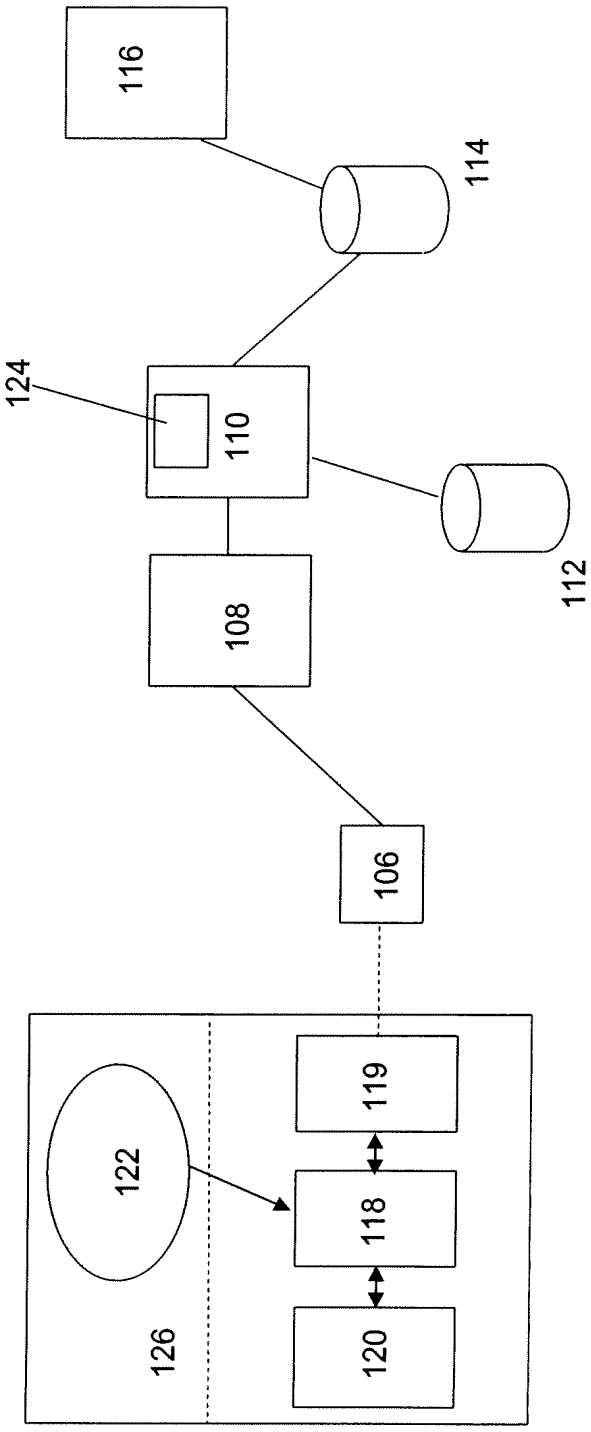


Figure 1

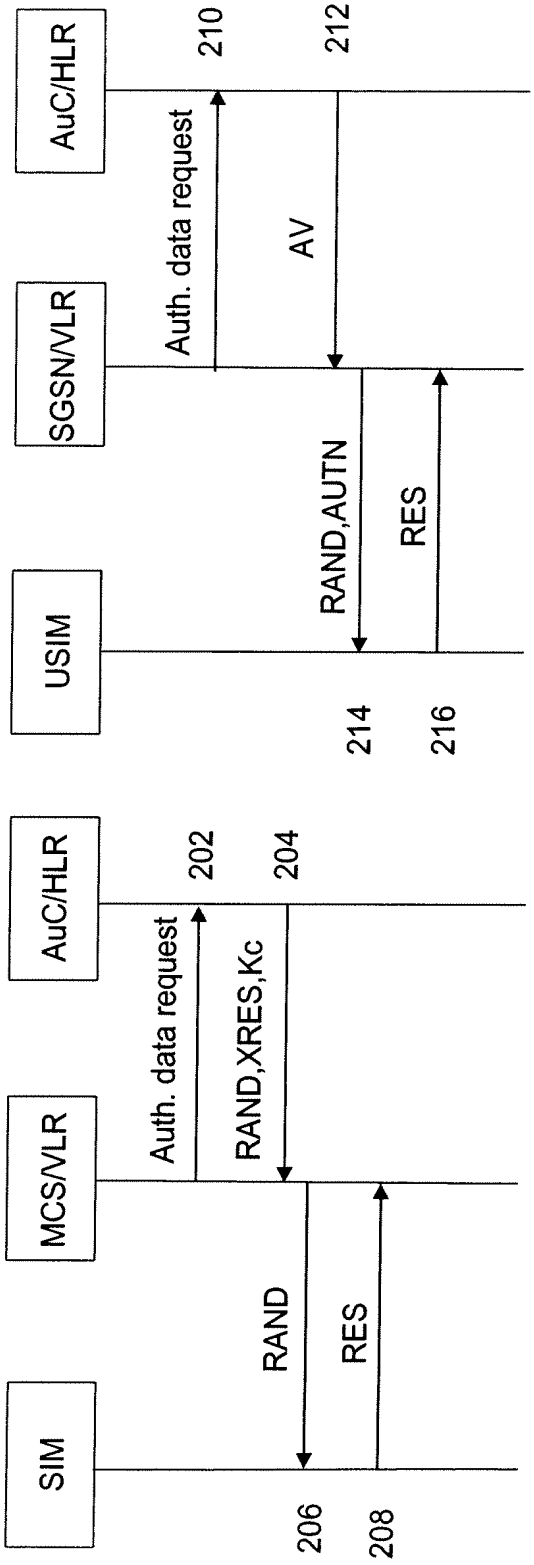

AuC/HLR
SGSN/VLR
USIM
Auth. data request
AV
RAND,AUTN
RES
210
212
214
216
(b)
AuC/HLR
MCS/VLR
SIM
Auth. data request
RAND,XRES,Kc
RAND
RES
202
204
206
208
(a)
200

Figure 2

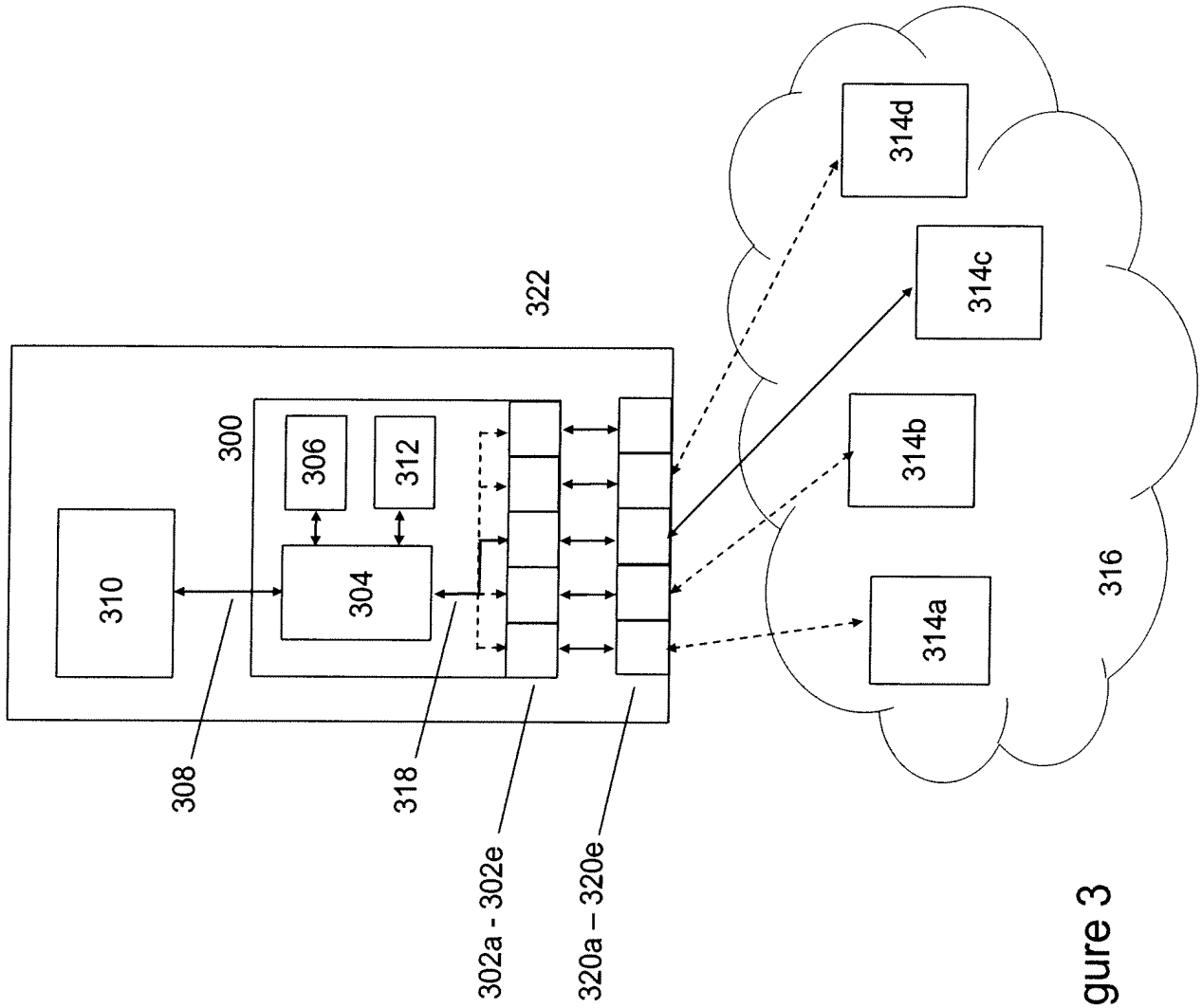

322
300
306
312
310
304
308
318
302a - 302e
320a – 320e
314d
314c
314b
314a
316

Figure 3

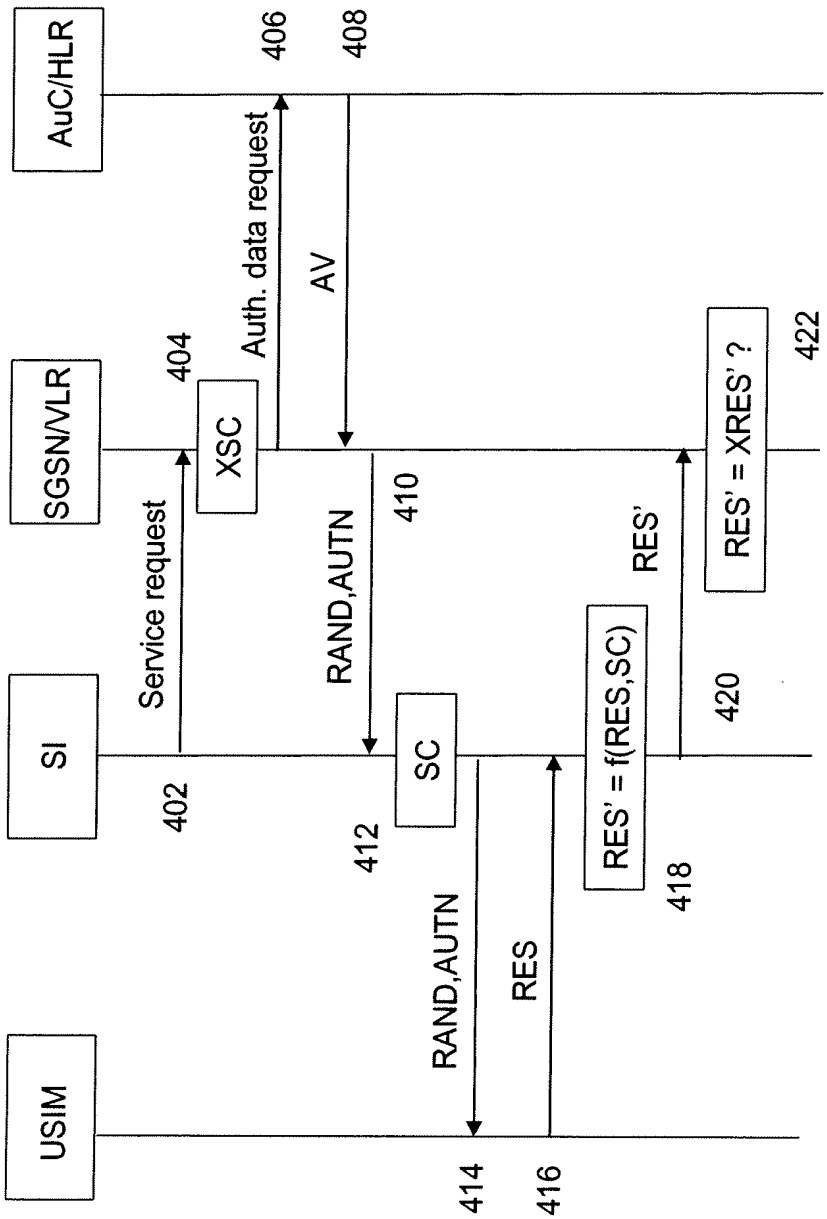

AuC/HLR
SGSN/VLR
SI
USIM
406
408
404
Auth. data request
AV
XSC
Service request
RAND,AUTN
410
SC
RES' = f(RES,SC)
RES'
RES' = XRES' ?
422
420
402
412
418
RAND,AUTN
RES
414
416
400

Figure 4

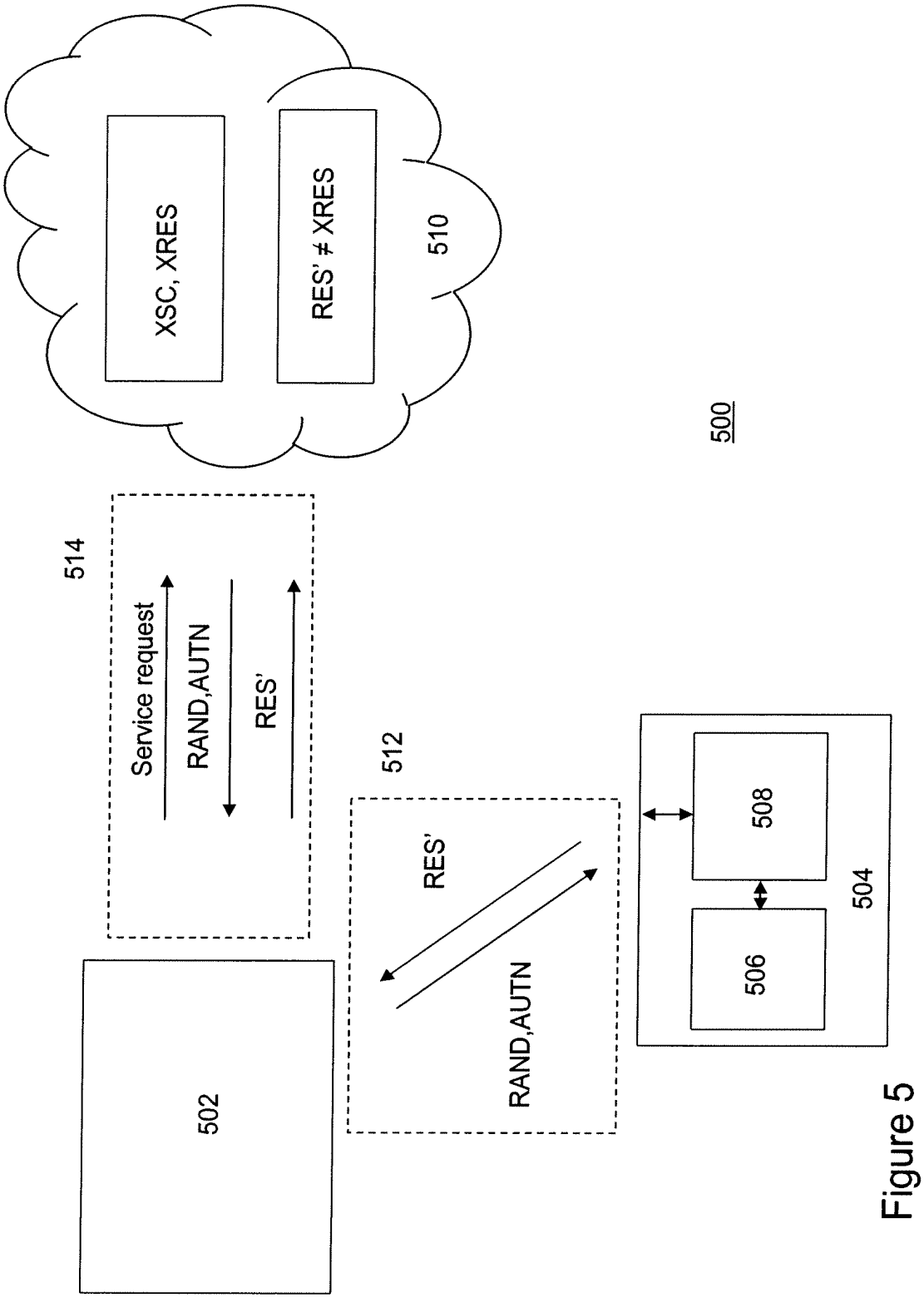

XSC, XRES
RES' ≠ XRES
510
500
514
Service request
RAND,AUTN
RES'
512
RES'
RAND,AUTN
508
506
504
502

Figure 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/067201

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06

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)
H04W H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/288407 A1 (NASLUND MATS [SE] ET AL) 21 December 2006 (2006-12-21)	1,3-5, 8-12,14, 16,18
Y	paragraph [0003] paragraphs [0006] - [0009] paragraph [0014] paragraph [0024] paragraphs [0035], [0036] paragraphs [0056] - [0064] paragraphs [0074] - [0077] paragraphs [0084] - [0087]; table 1 paragraphs [0099] - [0102] paragraphs [0108] - [0113]	2,6-7, 13,15,17

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family 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
19 February 2010	26/02/2010

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, Fax: (+31-70) 340-3016	Ruiz Sanchez, J

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/228992 A1 (MIZIKOVSKY SEMYON B [US]) 13 October 2005 (2005-10-13) paragraph [0017]; figure 1 paragraphs [0024] - [0031]; figure 3	1,3-5, 8-12,14, 16,18
Y	ERICSSON: "How to mitigate the Interleaving attack and reduce the trust in the Authenticator (S3-030084)" 3GPP TSG SA WG3 SECURITY, February 2003 (2003-02), XP050243902 the whole document	2,6-7, 13,15,17

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/067201

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006288407 A1	21-12-2006	NONE	
US 2005228992 A1	13-10-2005	NONE	

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
KONINKLIJKE KPN N.V.
Attn. Wuyts, Koenraad
P.O. Box 95321
NL-2509 CH The Hague
PAYS-BAS

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 403332WO	Date of mailing *(day/month/year)* 26/02/2010
International application No. PCT/EP2009/067201	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
Applicant KONINKLIJKE KPN N.V.	International filing date *(day/month/year)* 15/12/2009

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority 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	Authorized officer Anita Rothenbücher

Form PCT/ISA/220 (July 2009) *(See notes on accompanying sheet)*

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims,description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Annex B).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, International Phase, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet or sheets containing a complete set of claims in replacement of all the claims previously filed must be submitted.

Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively in Arabic numerals (Section 205(a)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide.*

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims,description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Annex B).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, International Phase, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet or sheets containing a complete set of claims in replacement of all the claims previously filed must be submitted.

Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively in Arabic numerals (Section 205(a)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
403332WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/EP2009/067201	15/12/2009	15/12/2008
Applicant		
KONINKLIJKE KPN N.V.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/067201

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06

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)
H04W H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/288407 A1 (NASLUND MATS [SE] ET AL) 21 December 2006 (2006-12-21)	1,3-5, 8-12,14, 16,18
Y	paragraph [0003] paragraphs [0006] - [0009] paragraph [0014] paragraph [0024] paragraphs [0035], [0036] paragraphs [0056] - [0064] paragraphs [0074] - [0077] paragraphs [0084] - [0087]; table 1 paragraphs [0099] - [0102] paragraphs [0108] - [0113]	2,6-7, 13,15,17

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family 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
19 February 2010	26/02/2010

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, Fax: (+31-70) 340-3016	Ruiz Sanchez, J

1

Form PCT/ISA/210 (second sheet) (April 2005)

Samsung Ex. 1002, Page 250 of 341

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/228992 A1 (MIZIKOVSKY SEMYON B [US]) 13 October 2005 (2005-10-13) paragraph [0017]; figure 1 paragraphs [0024] - [0031]; figure 3	1,3-5, 8-12,14, 16,18
Y	ERICSSON: "How to mitigate the Interleaving attack and reduce the trust in the Authenticator (S3-030084)" 3GPP TSG SA WG3 SECURITY, February 2003 (2003-02), XP050243902 the whole document	2,6-7, 13,15,17

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/067201

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006288407 A1	21-12-2006	NONE	
US 2005228992 A1	13-10-2005	NONE	

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP2009/067201	15.12.2009	15.12.2008

International Patent Classification (IPC) or both national classification and IPC
INV. H04W12/06

Applicant
KONINKLIJKE KPN N.V.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office
P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tel. +31 70 340 - 2040
Fax: +31 70 340 - 3016

Date of completion of this opinion

see form PCT/ISA/210

Authorized Officer

Ruiz Sanchez, J

Telephone No. +31 70 340-4717

Form PCT/ISA/237 (Cover Sheet) (April 2005)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material:

      ☐ on paper

      ☐ in electronic form

   c. time of filing/furnishing:

      ☐ contained in the international application as filed.

      ☐ filed together with the international application in electronic form.

      ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2, 6-7, 13, 15, 17
	No:	Claims	1, 3-5, 8-12, 14, 16, 18
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-18
Industrial applicability (IA)	Yes:	Claims	1-18
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1 US 2006/288407 A1 (NASLUND MATS [SE] ET AL) 21 December 2006

D2 US 2005/228992 A1 (MIZIKOVSKY SEMYON B [US]) 13 October 2005

D3 ERICSSON: "How to mitigate the Interleaving attack and reduce the trust in the Authenticator (S3-030084)" 3GPP TSG SA WG3 SECURITY, February 2003

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1, 9, 11, 12, 14, 16, 18 is not new.

2.1 Document D1 discloses (the references in parentheses applying to this document) a method for service - based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting - up a communication channel with the network (figure 4, the mobile terminal comprises several communication units: e.g GSM, UMTS, Bluetooth...), the method comprising the steps of:

- sending a service request for access to a network service (this step is implicitly disclosed, since authentication in the services disclosed in D1, e.g. GSM, UMTS... is triggered as a response to an access request);

- receiving in response to the service request an authentication request from the network (paragraph [0084]: "AKA request");

- identifying the communication channel through which the authentication request was received (paragraph [0084], first sentence: "...the terminal (mobile) may be configured to determine whether the AKA request initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces"); and,

- sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel (paragraph [0084] and table 1: additional processing of the challenge/ response depends on the communication channel; paragraph [0110] shows the modification of the result parameter sent to the network).

2.2 The same reasoning applies mutatis mutandis to independent claims 9, 11, 12, 14, 16, 18. The subject-matter of claims 9, 11, 12, 14, 16, 18 is therefore not new.

2.3 For the sake of completeness, it is noticed that document D2 discloses dual terminals using the same identification module for authenticating the network access via two different network interfaces (paragraph [0025]) wherein the response of the terminal to the authentication request depends on the communication channel used. According to D2 the authentication information received from the network is treated differently depending on the access interface used: in the case of IS-2000, the standard challenge/response with CAVE is performed (paragraph [0025], third sentence), whereas in the case of HRPD, the authentication information is modified by the terminal before passing it to the identity module (paragraph [0027]) and the response received from the identity module is modified (paragraphs [0029] and [0030]). The corresponding modifications of the information received by the HLR/AuC are performed by the AAA in the network side (paragraph [0030]). Therefore, the subject-matter of claims 1, 9, 11, 12, 14, 16, 18 is also considered not new over disclosure D2.

2.4 The attention of the applicant is also drawn to the fact that commonly used USIM/SIM/ISIM modules fall into the scope of claim 11, since the modification of the standard response on the basis of a predetermined function and the identified communication channel are defined as optional.

3 Claims 2-8, 10, 13, 15, 17 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT with respect to novelty and/or inventive step:

3.1 The additional features of claims 3-5, 8, 10 are known from D1 (see point 2.1 above and the corresponding passages cited on the search report, in particular paragraphs [0024], [0036], [0056] and [0087]).

3.2 The additional features of claims 2, 6, 7, 13, 15, 17 are rendered obvious by the combination of documents D1 (see paragraphs [0020] and [0108] to [0111]) and D3 (see page 2, "solution 2", which teaches the use of a service identifier in the modified challenge/response to avoid that an attacker re-uses AKA quintets with a different service).

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information	For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.
Amending claims under Art. 19 PCT	Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.
Filing a demand for international preliminary examination	In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT). If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).
Filing informal comments	After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.
End of the international phase	At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).
Relevant PCT Rules and more information	Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

BNSDOCID: <XS_____ 200704010CK | >

Bitte beachten Sie, dass angeführte Nichtpatentliteratur (wie z. B. wissenschaftliche oder technische Dokumente) je nach geltendem Recht dem Urheberrechtsschutz und/oder anderen Schutzarten für schriftliche Werke unterliegen könnte. Die Vervielfältigung urheberrechtlich geschützter Texte, ihre Verwendung in anderen elektronischen oder gedruckten Publikationen und ihre Weitergabe an Dritte ist ohne ausdrückliche Zustimmung des Rechtsinhabers nicht gestattet.

Veuillez noter que les ouvrages de la littérature non-brevets qui sont cités, par exemple les documents scientifiques ou techniques, etc., peuvent être protégés par des droits d'auteur et/ou toute autre protection des écrits prévue par les législations applicables. Les textes ainsi protégés ne peuvent être reproduits ni utilisés dans d'autres publications électroniques ou imprimées, ni rediffusés sans l'autorisation expresse du titulaire du droit d'auteur.

Please be aware that cited works of non-patent literature such as scientific or technical documents or the like may be subject to copyright protection and/or any other protection of written works as appropriate based on applicable laws. Copyrighted texts may not be copied or used in other electronic or printed publications or re-distributed without the express permission of the copyright holder.

XS CPRTENFRDE

PATENT COOPERATION TREATY

ADVANCE E-MAIL

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

WUYTS, Koenraad
P.O. Box 95321
NL-2509 CH The Hague
PAYS-BAS

Date of mailing *(day/month/year)* 05 February 2010 (05.02.2010)	
Applicant's or agent's file reference 403332WO	**IMPORTANT NOTIFICATION**
International application No. PCT/EP2009/067201	International filing date *(day/month/year)* 15 December 2009 (15.12.2009)
International publication date *(day/month/year)* **Not yet published**	Priority date *(day/month/year)* 15 December 2008 (15.12.2008)
Applicant KONINKLIJKE KPN N.V. et al	

1. By means of this Form, which replaces any previously issued notification concerning submission or transmittal of priority documents, the applicant is hereby notified of the date of receipt by the International Bureau of the priority document(s) relating to all earlier application(s) whose priority is claimed. Unless otherwise indicated by the letters "NR", in the right-hand column or by an asterisk appearing next to a date of receipt, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. *(If applicable)* The **letters "NR"** appearing in the right-hand column denote **a priority document which, on the date of mailing of this Form, had not yet been received by the International Bureau** under Rule 17.1(a) or (b). Where, under Rule 17.1(a), the priority document must be submitted by the applicant to the receiving Office or the International Bureau, but the applicant fails to submit the priority document within the applicable time limit under that Rule, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

3. *(If applicable)***An asterisk (*)** appearing next to a date of receipt, in the right-hand column, denotes **a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b)** (the priority document was received after the time limit prescribed in Rule 17.1(a) or the request to prepare and transmit the priority document was submitted to the receiving Office after the applicable time limit under Rule 17.1(b)). Even though the priority document was not furnished in compliance with Rule 17.1(a) or (b), the International Bureau will nevertheless transmit a copy of the document to the designated Offices, for their consideration. In case such a copy is not accepted by the designated Office as the priority document, Rule 17.1(c) provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
15 December 2008 (15.12.2008)	08021705.2	EP	01 February 2010 (01.02.2010)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Yolaine Cussac
e-mail PT05.PCT@WIPO.INT
Telephone No. +41 22 338 74 05

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)
(Case No. 11-808-WO-US)

In re Application of:	)	
	)	
Franklin Selgert et al.	)	
	)	**Examiner: TBA**
Serial No.: Not yet assigned	)	
Int'l Appln. No.: PCT/EP2009/067201	)	**Art Unit: TBA**
	)	
Int'l. Filing Date: 15 December 2009	)	
	)	
For: Service-Based Authentication to a Network	)	

PRELIMINARY AMENDMENT

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

Dear Sir:

Prior to examination of the concurrently filed United States National application corresponding to PCT/EP2009/067201, Applicants respectfully request entry of the attached amendments to the specification beginning on page 2 and the claims beginning on page 3, as well as consideration of the attached Remarks beginning on page 9.

AMENDMENT TO THE SPECIFICATION

In the first page, after the Title of the Invention, please insert the following:

"CROSS REFERENCE TO RELATED APPLICATIONS

The present application is a national stage entry of PCT/EP2009/067201, filed December 15, 2009, and claims priority to EP 08021705.2, filed December 15, 2008, the entire contents of which is incorporated herein by reference."

Samsung Ex. 1002, Page 262 of 341

AMENDMENTS TO THE CLAIMS:

1. (Currently amended) Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising ~~the steps of~~:

- sending a service request for access to a network service;
- receiving in response to the service request an authentication request from the network;
- identifying the communication channel through which the authentication request was received; and,
- sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

2. (Currently amended) Method according to claim 1, the method further comprising ~~the steps of~~:

- determining a service code associated with the identified communication channel;
- calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information regarding the identity of the communication channel through which the authentication request was received into the response.

3. (Currently amended) Method according to claim[[s]] 1 ~~or 2~~, wherein the terminal comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.

Samsung Ex. 1002, Page 263 of 341

4. (Currently amended) Method according to claim 1 ~~any of claims 1 to 3~~, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising ~~the steps of~~:

- modifying the authentication information on the basis of the identified communications channel;
- generating, preferably using an authentication and key agreement (AKA) of a telecommunication standard, an authentication response RES on the basis of the modified authentication information.

5. (Currently amended) Method according to claim 1 ~~any of claims 1 to 3~~, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising ~~the steps of~~:

- generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication standard, an authentication response RES;
- modifying, preferably using a one-way function, the authentication parameter RES on the basis the identified communications channel.

6. (Currently amended) Method according to claim 2 ~~any of claims 2-5~~, the method further comprising ~~the steps of~~:

- the terminal sending a service request via a predetermined communications channel to the network;
- the network generating an expected service code XSC on the basis of the type of communications channel the service request was sent to the network; and
- determining on the basis of expected service code XSC an expected response XRES.

7. (Currently amended) Method according to claim 6, the method further comprising ~~the steps of~~:

- comparing the expected response XRES with the authentication response RES send by the terminal to the network; and[[,]]

– determining the terminal to be in an un-trusted state if RES is not equal to XRES.

8. (Currently amended) Method according to claim 1 ~~any of claims 1-7~~, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

9. (Original) Service interface module for use in a terminal, preferably configured to securely process all authentication information transmitted to and from an identity module in the terminal, the service interface module comprising:

– a receiver for receiving an authentication signal from the network via one of the communications interfaces of the terminal;

– a channel identifier for identifying the communication channel through which the authentication signal was received, preferably by providing a service code associated with the identified communication channel;

– a channel interface for establishing a secure communication channel between the module and an identity module of the terminal.

10. (Original) Service interface module according to claim 9, the module further comprising:

– a modifier for modifying an authentication response of the identity module on the basis of the identified communication channel, or means for transmitting information regarding the identified communications channel to the identity module, or means for modifying the authentication signal received from the network.

11. (Currently amended) An identity module, preferably a smartcard, for establishing a safe communication channel with a service interface module as claimed in claim[[s]] 9 ~~or 10~~, the identity module comprising: a calculator for calculating a response RES

Samsung Ex. 1002, Page 265 of 341

- preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA
- upon receipt of an authentication request; and, optionally, a modifier for modifying the response RES on the basis of a predetermined mathematical function using information on the identified communication channel.

12. (Currently amended) A terminal, preferably a mobile device, for accessing network services, the terminal ~~being~~ configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal.

13. (Currently amended) The terminal as recited in claim 12 wherein the terminal is configured to:

- receive an authentication request from the network;
- determine a service code associated with the type of communication channel via which the authentication request was received by the terminal; and[[;]]
- send in response to the authentication request an authentication response RES to the network wherein the authentication response depends on the determined service code.

14. (Currently amended) A network node for service-based authentication of a terminal to a network, the network node ~~being~~ configured to generate in response to the receipt of an authentication data request a modified expected response XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

Samsung Ex. 1002, Page 266 of 341

15. (Currently amended) A network node as recited in claim 14, wherein the network node is configured to:

- receive an authentication data request;
- determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network; and[[;]]
- generate in response to the receipt of the authentication data request an expected response XRES, wherein the expected response depends on the determined expected service code.

16. (Original) A system for service based authentication to a network, comprising:

- a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal;
- a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

17. (Currently amended) A system as recited in claim 16, comprising:

- a terminal configured to receive an authentication request from the network, to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal and to send in response to the authentication request an authentication response RES to the network wherein the authentication response depends on the determined service code; and[[;]]
- a network node configured to receive an authentication data request, determine an expected service code associated with the type of communication channel via which the

Samsung Ex. 1002, Page 267 of 341

authentication data request was received by the network and to generate in response to the receipt of the authentication data request an expected response XRES, wherein the expected response depends on the determined expected service code.

18. (Currently amended) A computer program product comprising software code portions configured for, when run in the memory of a terminal, preferable a mobile device, executing the method ~~steps~~ according to claim 1. ~~any of claims 1-5.~~

Samsung Ex. 1002, Page 268 of 341

REMARKS

No new matter has been introduced into the present application as a result of the above amendments.

Applicant submits this preliminary amendment to put the claims in better condition for examination. Prompt consideration and entry of this amendment prior to examination is respectfully requested. If there are any questions or comments regarding this Amendment or application, the Examiner is encouraged to contact the undersigned attorney as indicated below.

Respectfully submitted,

Date: June 13, 2011

/Scott M. Miller/
Scott M. Miller
Reg. No. 62,967

McDonnell Boehnen Hulbert & Berghoff LLP
300 South Wacker Drive
Chicago, IL 60606

Telephone: 312-913-0001
Facsimile: 312-913-0002

Samsung Ex. 1002, Page 269 of 341

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Franklin Selgert
Filer:	Scott Michael Miller
Attorney Docket Number:	11-808-WO-US

Filed as Large Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
National Stage Fee	1631	1	330	330
Natl Stage Search Fee - Report provided	1642	1	430	430
National Stage Exam - all other cases	1633	1	220	220
Pages:				
Claims:				
Independent claims in excess of 3	1614	2	220	440
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1420**

Electronic Acknowledgement Receipt

EFS ID:	10289600
Application Number:	13139433
International Application Number:	PCT/EP09/67201
Confirmation Number:	1414
Title of Invention:	Service-Based Authentication to a Network
First Named Inventor/Applicant Name:	Franklin Selgert
Customer Number:	20306
Filer:	Scott Michael Miller
Filer Authorized By:	
Attorney Docket Number:	11-808-WO-US
Receipt Date:	13-JUN-2011
Filing Date:	
Time Stamp:	15:55:40
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1420
RAM confirmation Number	2380
Deposit Account	132490
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. 1.492 (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)

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	Transmittal of New Application	11_808_WO_US_Transmittal.pdf	522932 c1d9daf2d7ce8ce881c60cf30279b42910d3e4d1	no	4
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	11_808_WO_US_IDS.pdf	612452 9a7d9a1a1f904b1c55df8f774ccd6c3e1d3244ea	no	4
Warnings:					
Information:					
3	Non Patent Literature	NPL_1.pdf	576238 a6ec492431b1fc3c103ddc1324755bbf222c1c5f	no	14
Warnings:					
Information:					
4	Non Patent Literature	NPL_2.pdf	121336 e15abbc228f11470f9aa4163d74eeadf4c3de643	no	4
Warnings:					
Information:					
5	Non Patent Literature	NPL_3.pdf	298423 10fd096ac70ffe22aac5357d6ca2c3b13f2f910c	no	9
Warnings:					
Information:					
6	Application Data Sheet	11_808_WO_US_ADS.pdf	1031785 10f7e624604629518cee355c6a9be2d3d7a7a2f3	no	5
Warnings:					
Information:					
7	Documents submitted with 371 Applications	PCTEP2009067201.pdf	1517514 a9bbd4584e9524b100114b69b13a1e3fa3a0b0a7	no	34
Warnings:					
Information:					
8	Documents submitted with 371 Applications	11_808_WO_US_Search_Report_Written_Opinion.pdf	576237 97b8ffcd8ef43f06182e2257bc694ee15573b798	no	14

Warnings:					
Information:					
9	Documents submitted with 371 Applications	PCTIB304_Form.pdf	10882 c6c74651ac021098dbe8ba902bec87b3e6994164	no	1
Warnings:					
Information:					
10		11-808-WO-US_Pre_Amend.pdf	106479 0da7044f0e35aaa2f9ebf46301755aac3541b92f	yes	9

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Specification	2	2
Claims	3	8
Applicant Arguments/Remarks Made in an Amendment	9	9

Warnings:					
Information:					
11	Fee Worksheet (SB06)	fee-info.pdf	36365 68a4b66035f80cf9c4798d1c0491911442a3e509	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	5410643		

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.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 June 2010 (24.06.2010)

PCT

(10) International Publication Number
WO 2010/069962 A1

(51) International Patent Classification:
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/EP2009/067201

(22) International Filing Date:
15 December 2009 (15.12.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08021705.2 15 December 2008 (15.12.2008) EP

(71) Applicants *(for all designated States except US)*: **KONINKLIJKE KPN N.V.** [NL/NL]; Maanplein 55, NL-2516 CK The Hague (NL). **NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO** [NL/NL]; Schoemakerstraat 97, NL-2628 VK Delft (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SELGERT, Franklin** [NL/NL]; Penningslaan 30, NL-2651 BL Berkel en Rodenrijs (NL). **MULLER, Frank** [NL/NL]; Hopstraat 39, NL-2611 TB Delft (NL).

(74) Agent: **WUYTS, Koenraad**; P.O. Box 95321, NL-2509 CH The Hague (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: SERVICE-BASED AUTHENTICATION TO A NETWORK

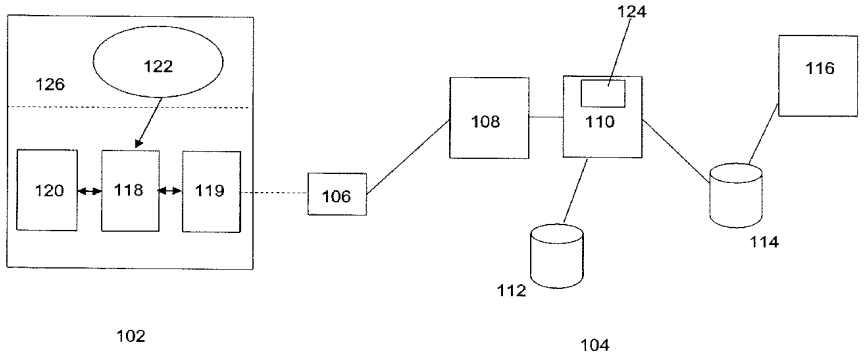


Figure 1

(57) **Abstract**: A method and a system for service-based authentication of a terminal to a network is described, wherein the terminal comprises a number of communications interfaces, each communications interface allowing the terminal to set-up a predetermined communication channel with the network. The method comprises the steps of: sending a service request for access to a network service; receiving in response to the service request an authentication request from the network; identifying the communication channel through which the authentication request was received; and, sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

WO 2010/069962 A1

Service-based authentication to a network.

Field of the invention

The invention relates to a service-based authentication to a network and, in particular, though not exclusively, to a method and a system for a service-based authentication of a terminal to a network and a service interface module for use in such system.

Background of the invention

The new generation mobile devices, such as smart phones, provide more and more enhanced computational functionalities via open network connections. Such mobile devices are e.g. capable of receiving e-mail, share software with one another through short-range connections, downloading and executing software from the Internet, making automated calls and act under remote control. Hence, similar to a personal computer, mobile devices and in particular the software components involved in the setting up of a connection between the mobile device to the network, are vulnerable to attacks of malicious code (malware). Typically malware attempts to make misuse of mobile device or to simply disrupt legitimate use of a mobile device.

Typically, malware makes use of security flaws in the authentication procedure which provides a subscriber access to a network. For example the GSM authentication and key agreement (AKA) only authenticates the mobile device to the network, but not the other way around. The GSM AKA is therefore vulnerable to so-called false base station attacks wherein an attacker pretends to be a valid base station. In the UMTS AKA part of these threats are mitigated by using a mutual authentication wherein the mobile device has to authenticate itself to the Visitor Location Register (VLR) and the VLR has to authenticate itself to the mobile device. An overview of the security threats in the GSM AKA and the way a

number of these threats are counteracted by the UMTS AKA are described in ETSI TS 33.900.

From TS 33.900 it follows that the UMTS AKA is still vulnerable to security attacks. For example, the UMTS AKA is vulnerable to the so-called man-in-the-middle attacks, wherein a mobile device of an attacker may use authentication information from the (U)SIM of the victim in order to obtain access to the network. Such a man-in-the-middle attack allows network access as if the connection was set up by the victim. As the network cannot distinguish between a legal situation and such attack the malware allows to set up calls on the expenses of the victim thereby causing substantial damage.

Summary of the invention

It is an object of the invention to reduce or eliminate at least one of the drawbacks known in the prior art and to provide in a first aspect of the invention a method for service-based authentication of a terminal to a network. The terminal comprises one or more communications interfaces for allowing the terminal to setting-up a communication channel with the network. The method comprises the steps of: sending a service request for access to a network service; receiving in response to the service request an authentication request from the network; identifying the communication channel through which the authentication request was received; and, sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

The method allows the network to determine through which communication channel authentication information is transmitted to the network. Determination of the communication channel can be easily achieved by identifying the communication interface through which the authentication request is received. Such service-based authentication method effectively prevents misuse of authentication information, e.g. a man-in-the-middle attack wherein an attacker uses

authentication information from the (U)SIM of the victim in order to obtain access to the network.

Furthermore, the method is compatible with all or at least most existing and proposed AKA's. It only requires determination of the communication channel through which the request was received and secure insertion of information regarding the communication channel into the response.

In one embodiment the method further comprises the steps of: determining a service code associated with the identified communication channel; calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information regarding the identity of the communication channel through which the authentication request was received into the response.

The information regarding the communication channel through which the authentication information is transmitted to the network is securely inserted in the response of the identity module of the terminal. Hence, it is not possible or at least very difficult for malware to detect and/or modify the service channel information.

In another embodiment the terminal used in the method comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.

By using a service interface module as a trusted hardware module in the terminal, a very safe and reliable method is achieved for sending the information regarding the identity of the communication channel to the network. Preferably, the service interface module is configured to receive all incoming authentication signals from the network. Hence, all authentication request will be routed via the service interface module to the identity module of the terminal.

In yet another embodiment the authentication request comprises authentication information, preferably a random

challenge RAND and the method further comprises the steps of: modifying the authentication information on the basis of the identified communications channel; generating, preferably using an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES on the basis of the modified authentication information.

In one embodiment the authentication request comprises authentication information, preferably a random challenge RAND and the method further comprises the steps of: generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES; modifying, preferably using a one-way function, the authentication parameter RES on the basis the identified communications channel.

This embodiment allows simple and safe implementation of the method by using a service interface module which securely communicates with the identity module. Identification of the communication channel and secure insertion of the information regarding the identified communication channel may take place in the service interface module so that no modifications of the identity module are required. This implementation is thus compatible with existing identity modules.

In another embodiment the method further comprises the steps of: the terminal sending a service request via a predetermined communications channel to the network; the network generating an expected service code XSC on the basis of the type of communications channel the service request was sent to the network; determining on the basis of expected service code XSC an expected response XRES.

In one embodiment the method further comprises the steps of: comparing the expected response XRES with the authentication response RES send by the terminal to the network; and, determining the terminal to be in an un-trusted state if RES is not equal to XRES.

Hence, the method only requires a simple modification in the existing network in the sense that it requires a network node which is configured to identify the communication channel through which the service request is received by the network and to extract the information regarding the communication channel encrypted in the terminal response.

In one embodiment the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

In a further aspect the invention relates to a service interface module for use in a terminal, preferably configured to securely process all authentication information transmitted to and from an identity module in the terminal, wherein the service interface module comprises: a receiver for receiving an authentication signal from the network via one of the communications interfaces of the terminal; a channel identifier for identifying the communication channel through which the authentication signal was received, preferably by providing a service code associated with the identified communication channel; an interface for establishing a secure communication channel between the module and an identity module of the terminal.

All functionality required in the terminal for implementation of the method can be simply located in one trusted hardware module which securely communicates with the identity module.

In one embodiment the service interface module further comprises a modifier for modifying an authentication response of the identity module on the basis of the identified communication channel, or sender for transmitting information regarding the identified communications channel to the identity module, or modifier for modifying the authentication request received from the network.

In another aspect the invention relates to an identity module, preferably a smartcard, for establishing a safe communication channel with a service interface module as described above. The safe communication channel may for

example consist of a link protected with cryptography or a direct hardware link between the service interface module and the identity module that cannot be interfered with by an attacker. The identity module comprises: a calculator for calculating a response RES - preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA - upon receipt of an authentication request; and, optionally, a modifier for modifying the response RES on the basis of a predetermined mathematical function using information on the identified communication channel.

In yet another aspect the invention relates to a terminal, preferably a mobile device, for accessing network services, wherein the terminal is configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal.

In one embodiment the terminal comprises a service interface module according as described and, optionally, an identity module as described above.

In a further aspect the invention relates to a network node for service-based authentication of a terminal to a network, wherein the network node is configured to generate in response to the receipt of an authentication data request a modified expected response XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

In one embodiment the network node comprises: a receiver for receiving a service request from a terminal; a generator for generating an expected service code XSC on the basis of the type of communication channel the service request was sent to the network; a generator for generating an expected response XRES or a receiver for receiving from another network node an expected response XRES, preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA; and, a modifier the expected response XRES on the basis of a predetermined mathematical function, preferably a one-way

function, using the expected service code XSC as an input parameter.

In one embodiment the network node further comprises: a receiver for receiving a response RES from a terminal; a comparator for comparing the response RES with the modified expected response XRES'.

In yet a further aspect the invention relates to a system for service based authentication to a network, comprising: a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal; and, a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

The invention also relates to a computer program product comprising software code portions configured for, when run in the memory of a terminal, preferable a mobile device, executing the method steps as described above.

The invention will be further illustrated with reference to the attached drawings, which schematically will show embodiments according to the invention. It will be understood that the invention is not in any way restricted to these specific embodiments.

Brief description of the drawings

Fig. 1 depicts a schematic representation of a system according to one embodiment of the invention.

Fig. 2 illustrates a schematic flow diagram of the GSM authentication procedure and the UMTS authentication procedure.

Fig. 3 depicts the service interface module according to one embodiment of the invention.

Fig. 4 depicts a flow diagram according to one embodiment of the invention.

Fig. 5 illustrates prevention of a fraudulous authentication procedure by using the invention.

Detailed description

Fig. 1 illustrates a schematic representation of a communications system **100** according to one embodiment of the invention. The system comprises a terminal **102** connected to a communications network **104**. In one embodiment the network may be a 2G-type (e.g. GSM) mobile network comprising a base transceiver station (BTS) **106** serving as an access node. The BSC is connected via a base station controller (BSC) **108** to a mobile switching center (MSC) **110** of e.g. a visiting network (VN). The MSC is linked to a visited location register (VLR) **112**, which is a database that stores user related data and performs security functions. The MSC is further linked to a home location register (HLR) **114** which is located in the home network (HN) where the user of the terminal **102** has a subscription with the network operator. The HLR **114** stores user related data, e.g. subscription related data, and co-operates with the MSC/VLR **110** to keep track of the location of the terminal. The HLR is connected to an authentication centre (AuC) **116**. The authentication centre (AuC) comprises (amongst others) algorithms for the calculation of authentication parameters used in the authentication procedure. For each subscriber the AuC stores a secret authentication key K which is also stored in an associated identity module, e.g. a (U)SIM card or the like, located in the terminal.

Alternatively, the network in Fig. **1** may also depict a 3G-type (e.g. UMTS) mobile network comprising 3G network elements. In that case, the network may comprise a radio base station (Node-B) **106** connected via a Radio Network Controller (RNC) **108** to a Serving GPRS Support Node (SGSN) **110**. The SGSN is further connected to a VLR **112** and an AuC/HLR **114,116** in a similar way as in the 2G-type network as described above.

In a further embodiment the communications network **104** may comprise IMS-based network elements in the form of a set of Call/Session Control Functions (CSCF) such as a Proxy-CSCF (P-CSCF), an Interrogating-CSCF (I-CSCF), a Serving-CSCF (S-CSCF) and a Home Subscriber Server (HSS). In yet further embodiments the communications network may comprise 3GPP LTE or 3GPP SAE network elements.

The terminal **102** may be a personal computer or a mobile device such as a smart phone, a personal digital assistant (PDA), a laptop or any other mobile communications device capable of providing services over one or more networks. The terminal comprises a service interface (SI) module **118**, an operating system (OS) **126** and an identity module **120**.

The SI module **118** acts as a central access point to wired and wireless network services and comprises for that purpose a number of service interfaces. For example, for wireless services, it includes an interface to an RF module, e.g. a 2G or 3G radio card, comprising an RF receiver connecting to one more antennas. **Fig. 1** depicts an exemplary implementation wherein a radio card module **119** provides radio contact with the base station **106**. The RF interface of the radio card is capable of receiving and/or transmitting RF signals in accordance with various wireless technologies using licensed frequency bands (e.g. TDMA for GSM services or W-CDMA for UMTS services). The radio card must have a secure interface to the SI module. Beside the interface to the RF module the SI module may comprise a number of interfaces to other wireless interface modules, e.g. wireless interface modules using non-licensed frequency bands such as the IEEE 802.11 interface for WLAN services, the IEEE 802.15.1 interface for Bluetooth services, an DECT interface as described in ETS 300 175, etc.

The SI module may also comprise interfaces to one or more wired interface modules, e.g. an Ethernet interface allowing the SI module to be connected to the network using a wired Ethernet communication channel. An access and configuration (AC) manager in the SI module manages the set-up

of a communication channel to an access node of a network or - in case of a short-range connection such as Bluetooth - to another terminal. It determines the correct parameter for operation under a specific wired or wireless technology and/or protocol associated with the networks services requested by the terminal. Further, the SI module is configured to securely include information regarding the used interface in the data sent to a Service Identification Unit (SIU) **124** in the network. The interaction between the SI module **118** and the SIU **124** is explained hereunder in more detail.

The Operating System (OS) of the terminal comprises a kernel which manages the resources of the mobile device e.g. the Central Processing Unit (CPU), memory for storing program instructions and data and Input/Output (I/O) devices such as the radio module. Further, the OS comprises Application Programming Interfaces (APIs) through which application programs **122** may access services offered by the OS. The OS may comprise APIs for setting up wired or wireless connections via one of the interfaces modules.

The identity module **120**, which is typically removable, may be a UICC (Universal Integrated Circuit Card) for use in mobile devices suitable for 2G-type network services (GSM) or 3G-type network services, (UMTS). To that end, the UICC may comprise a Subscriber Identity Module (SIM) application comprising SIM functions and/or a UMTS Subscriber Identity Module (USIM) application comprising USIM functions. It is to be understood that the identity module is not limited to SIM and/or USIM applications. In further embodiments, the identity module may be an IP Multimedia Sub-system SIM (ISIM) for authenticating and accessing IMS-based services according to a predetermined IMS-based AKA as e.g. described in ETSI technical specification TS 33.203 or an extensible authentication protocol (EAP) based SIM for authentication and accessing a network according to a predetermined EAP-based AKA as described for instance in RFC4187.

The identity module may comprise a processor, one or more memory components e.g. ROM, RAM and/or EEPROM and I/O circuitry. For authentication purposes the UICC comprises a

secret service-subscriber authentication key K and one or more algorithms for calculating a response comprising one or more authentication parameters upon the reception of a random challenge.

Fig. 2(a) illustrates a schematic flow diagram of the standard GSM authentication procedure which may be used by the SIM module in the identity module. In the GSM standard the MSC initiates, in response to a service request of a network service originating from the terminal, a request for authentication data to the AuC/HLR (step **202**). A random number generator at the AuC/HLR generates a random value RAND that is input to the GSM A3/A8 algorithms which generate an expected response XRES and a cipher key K_C. The triplet {RAND, XRES, K_C} is returned to the MSC (step **204**) that subsequently forwards the RAND value to the SIM card of the terminal (step **206**). Corresponding calculations are performed by the terminal, typically by the integrity module, which returns a calculated response RES back to the MSC (step **208**). By comparison of the RES with the XRES the MSC can authenticate the terminal to the network.

In the standard UMTS authentication procedure similar steps as the GSM procedure are performed. However, in order to improve the security additional parameters and a set of eight functions f0-f5,f1*,f2* are used. **Fig. 2(b)** illustrates a schematic flow diagram of the UMTS authentication procedure, which may be used with a USIM application in the identity module. In response to a request for authentication data from the SGSN/VLR (step **210**), the AuC/HRL generates a random number RAND (using function f0) and a fresh sequence number SQN. The AuC/HRL provides the secret authentication key K (which is both stored in the AuC and the USIM but never directly exchanged) and an operator specific Authentication Management Field AMF. These four parameters are fed into the five symmetric encryption functions f1-f5, resulting in five new parameters: the Message Authentication Code (MAC), the Expected Response (XRES), the Ciphering Key (CK), the Integrity Key (IK) and the Anonymity Key (AK). The sequence number SQN is separately encrypted into SQN^1.

The AuC/HLR returns these parameters in an authentication vector (AV) {AUTN,RAND,XRES,CK,IK} to the SGSN/VLR (step **212**) wherein the Authentication token AUTN is a triplet {SQN^1,AMF,MAC}. Thereafter, the SGSN/VLR forwards an Authentication and Ciphering request comprising RAND and AUTN to the mobile device (step **214**). Using RAND and AUTN the USIM calculates - amongst others - a response RES, which is sent back to the SGSN (step **216**) and compared with the XRES as received from the AuC/HLR.

The keys for ciphering and integrity checking have a limited lifetime to prevent attempts to break the cipher or integrity protection by brute force long duration monitoring attacks. Upon expiry, a new set of ciphering and integrity keys are generated with a re-authentication between the terminal and the network. This re-authentication process is regularly repeated.

The GSM AKA is described in detail in ETSI standards GSM 02.09 and GSM 03.20 and the UMTS AKA described in detail in ETSI technical specification TS 33.102, which are hereby incorporated by reference.

Fig. 3 depicts an SI module according to a preferred embodiment of the invention The SI module **300** is located in a terminal **322** and comprises a number of interfaces **302a-302e**, which are connected, preferably through one or more secure communication channels , to associated interface modules **320a-320e**. The interface modules are located in the terminal and used for setting up a network connection with the network **316**. The SI module is configured to generate a service code (SC) identifying the specific service interface used to set up a wired or a wireless communication channel. To that end, the AC manager **304** in the SI module may use a look-up table **306** comprising the different types of service interfaces supported by the mobile terminal and the associated service codes. The AC manager may be implemented in the form of a processor and one or more memory modules comprising e.g. the configuration data of the look-up table.

The hardware of the terminal is preferably configured in such a way that all incoming authentication requests for a

network service received by one of the interfaces **302a-302e** will be centrally routed via the SI module to the UICC connected to the SI module. Such hardware architecture ensures that all incoming authentication requests are identified with respect to the communication channel the request was received by the terminal. Further, the SI module is configured to provide a secure communication channel **308** with the UICC **310** connected to the SI module. Hence, preferably, the SI module is implemented in the form of one or more trusted hardware components.

If, for example, the terminal **322** receives a network signal, e.g. a 3G signal, via a 3G RF interface module **320c** and the 3G interface **302c** of the SI module, the signal is translated into a digital signal in accordance with the technical specifications of the wireless air interface. Thereafter the digital signal comprising the authentication request is transmitted via the SI module to the UICC **310**. Further, the AC manager **304** identifies the service code associated with the 3G RF interface **302c** using a look-up table **306**. The service code is used by the SI module to provide the network with information regarding the origin of the authentication request.

The UICC processes the authentication request according to an AKA of a telecommunications standard, e.g. a GSM AKA or a UMTS AKA as described in relation with **Fig. 2** and then returns a response RES back to the SI module. Thereafter, the SI module uses a predetermined mathematical algorithm f stored in a secure memory **312** of the SI module in order to securely include the information embodied in the service code into the response RES received from the UICC. Preferably, the mathematical algorithm f is a so-called one-way function which is easy to compute but impossible or very hard to invert. A suitable one-way function may be a secure hash operation with the SC. Inserting the service code into the response allows the SI module to inform the network **316** about the communication channel (Bluetooth **314a**, WLAN **314b**, 3G **314c**, Ethernet **314d**, etc.) through which the authentication request

was received from the network in a way which is not, or at least very difficult, to modify by malware.

In order for the network to extract the channel information, the network, preferably the SGSN/VLR or an equivalent network node such as the MCS/VLR, comprises an Service Identification Unit (SIU). The SIU comprises a function f which is identical to the function f used by the SI module. Further, the SIU is configured to determine through what type of communication channel a service request is received.

The advantage of the architecture of the SI module as depicted in **Fig. 3** is that the specifications of the (U)SIM do not require changes. The implementation is simple and only requires the installation of a SI module in the terminal and a SIU in the network. Moreover, the architecture is backwards compatible with conventional equipment, i.e. terminals and network nodes (e.g. SGSN/VLR or MCS/VLR) which do not comprise a SI mode or a SIU.

A more detailed explanation on the functioning of the SIU will be given in relation to **Fig. 4**.

Fig. 4 depicts a process flow **400** between a UMTS network and a terminal comprising a USIM and an SI module as described in relation with **Fig. 1** and **3**. The process is started by a terminal application requesting a UMTS service from the network. The request triggers the RF interface module to set-up up a wireless UMTS communication channel between the terminal and an access node of the requested UMTS network. Thereafter, a service request is transmitted via the wireless communication channel to the SGSN/VLR (step **402**).

Then the SIU in the SGSN/VLR determines through which service interface (UMTS, GSM, WiFi, Bluethooth, etc.) contact was established with the terminal. On the basis of the identified service interface information an expected service code XSC is determined (step **404**). The SIU may determine XSC by retrieving the service code associated with the identified service interface (in this case a UMTS service) from a look-up table - substantially identical to the one used by the SI

module in the terminal - stored in a secure memory of the SI module.

In response to the service request, the SGSN/VLR sends an authentication data request to the AuC/HLR of the network (step **406**). The AuC/HLR generates a UMTS authentication vector AV, which is sent back to the SGSN/VLR (step **408**). Subsequently RAND and AUTN are sent in an Authentication and Ciphering request via the wireless communication channel to the terminal (step **410**). When the RF interface module of the terminal receives the radio signal comprising the request, the signal is converted to a digital signal. The AC manager identifies the service code associated with the interface used by the SI module to communicate with the RF module (step **412**). Thereafter, the digital signal comprising the RAND and AUTN is forwarded to the USIM (step **414**), which calculates the response RES using e.g. the f1-f5 algorithms of the UMTS AKA. Then the USIM sends the response RES back to the SI module (step **416**).

Using the SC and the one-way function f, the SI determines a modified response RES'=f(RES,SC) (step **418**), hence securely inserting information about the communication channel through which the request was received. This way, the response RES' becomes specific for the service it is meant for. The response RES' is subsequently transmitted back via RF interface to the SGSN/VLR in the network (step **420**) for comparison with an expected response XRES' (step **422**). The expected response XRES' may be determined by the SIU using the one-way function f with the expected response XRES determined on the basis of the UMTS AKA and the SC as the input parameters: XRES'=f(XRES,SC).

Thereafter a comparison between the terminal response RES' and the expected response XRES' is made. If RES' is equal to XRES' then this provides an indication for the network that the terminal received an authentication request via the communication channel that was expected by the network. In that case access to the network is granted.

If RES' is not equal to XRES' then an indication to the network is provided that the terminal received an

authentication request via a communication channel different from the communication channel expected by the network. This may provide the network with an indication that the terminal may be corrupted by malware.

It is noted that the invention is not limited to the embodiment as described in relation with **Fig. 3** and **4**. In a further embodiment the UICC (instead of the SI module) comprises the one-way function f for securely inserting the service code information into the response.

After the AC manager has selected the correct SC, the code is inserted into the digital signal comprising the request and send to the identity module for further processing (e.g. authentication and/or computation of the decryption key). Hence, in this variant the digital signal sent by the SI module to the identity module comprises information via which service interface (and hence via which communications channel) the signal was received. Further variants for sending the service code to the identity module may include, e.g. sending the service code to the identity module in a separate signal.

In one embodiment the (U)SIM may modify the authentication information in the authentication request, e.g. a random challenge RAND, on the basis of the service code SC and subsequently calculate a response RES on the basis of an authentication and key agreement (AKA) of a telecommunications standard. For example, in the case of a GSM service the SIM may perform the steps: RAND'=f(RAND,SC) and RES'=A3(RAND',K_C). In another variant, the SIM first calculates the response RES on the basis of the RAND and then modifies RES on the basis of SC: RES=A3(RAND,K_C) and RES'=f(RES,SC). In the case of an UMTS service, the f1-f5 algorithms of the UMTS AKA are used instead of the A3 algorithm of the GSM AKA.

Depending on the specific scheme implemented in the USIM, the SIU which comprises the mathematical function f used by the USIM in the terminal, may determine RAND'=f(RAND, XSC) and send this value to the AuC/HLR for determining the expected response XRES' on the basis the UMTS AKA using RAND' as one of the input parameters. Alternatively, the AuC/HRL may first determine XRES on the basis the UMTS AKA using RAND as

one of the input parameters and then send this value to the SIU for determining the expected response XRES'=f(XRES,XSC).

Fig. 5 represents a simplified schematic illustrating how a fraudulous authentication procedure may be prevented using the invention. In this scheme a first terminal **502** of an attacker remotely connects to an infected second terminal **504** of a victim and subsequently requests and uses authentication information from the (U)SIM **506** of the victim to obtain access to the network **510**.

The malware in the second terminal **504** allows the terminal of an attacker **502** to make a first communication channel **512**, e.g. a Bluetooth connection, with the infected terminal of the victim. Other types of connections such as a WiFi connection or a wired connection, such as an Ethernet connection, may also be possible. After connecting to the victim, the attacker starts an authentication procedure to the network by sending a service request via a second communication channel **514** to the AuC/HRL. In response, the attacker will receive an authentication request comprising - amongst others - RAND and AUTN. Instead of responding to the request, the attacker forwards the request to the victim using the Bluetooth connection to the (U)SIM of the victim .

A conventional (U)SIM cannot distinguish between requests originating from different communication channels (e.g. UMTS, GSM, WiFi, Bluetooth, etc.). In that case, the (U)SIM responds to the request by calculating a correct response RES, which is subsequently send via the Bluetooth connection (i.e. the communication connection where the request came from) to the network. The attacker may use this RES to authenticate itself successfully to the network. Using this mechanism the attacker is capable of correctly answering each subsequent Authentication and Ciphering Request from the network.

If however the network **510** and the infected terminal **504** in **Fig.5** are configured as a communications system according to the invention as described in relation with **Fig.1**, the SI module **508** is able to make a distinction between requests originating from different sources. In that case, the

network **510** will determine an expected service code XSC on the basis of the request of the attacker. As the attacker requested a UMTS service via second communication channel **514**, the network will set the XSC to the service code corresponding to a UMTS service. Similarly, the SI module **508** of the infected terminal will modify the RES using the service code corresponding to a Bluetooth communications channel **512**. This modified RES' is sent via the Bluetooth connection to the network, which will then determine that the XRES' calculated by the network on the basis of XSC does not match RES' because the communication channel used to send a request for a UMTS service to the network is different from the communication channel through which the terminal received the authentication request. In that case, the network may take appropriate action.

In one embodiment, the network may calculate the expected response values (XRES'', XRES''', etc.) for each service code available in the look-up table located in a service node of the network. If a XRES' value associated with a particular service code matches RES' then the source of the request received by the terminal may be determined.

This information may be used by the network to take appropriate action. It may e.g. provide no or limited access to the network or place the mobile device in a separate isolation or quarantine network in order to provide remediation services to the mobile device of the subscriber. If the response RES' is neither equal to XRES' nor to the other expected responses then the authentication procedure has failed.

It is to be understood that the invention may also be used with the IMS AKA (3GPP TS 33.203), in Generic Bootstrapping (GBA) applications (see 3GPP TS 33.220, 33.222, 33.223) or with the EAP AKA and/or EAP SIM in WLAN interworking applications. It can also be used in generic access solutions to the mobile network (see 3GPP TS 43.318).

Further, it is to be understood that any feature described in relation to any one embodiment may be used alone, or in combination with other features described, and may also

be used in combination with one or more features of any other of the embodiments, or any combination of any other of the embodiments. Furthermore, equivalents and modifications not described above may also be employed without departing from the scope of the invention, which is defined in the accompanying claims.

CLAIMS

1. Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising the steps of:
   - sending a service request for access to a network service;
   - receiving in response to the service request an authentication request from the network;
   - identifying the communication channel through which the authentication request was received; and,
   - sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

2. Method according to claim 1, the method further comprising the steps of:
   - determining a service code associated with the identified communication channel;
   - calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information regarding the identity of the communication channel through which the authentication request was received into the response.

3. Method according to claims 1 or 2, wherein the terminal comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.

4. Method according to any of claims 1 to 3, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising the steps of:

- modifying the authentication information on the basis of the identified communications channel;
- generating, preferably using an authentication and key agreement (AKA) of a telecommunication standard, an authentication response RES on the basis of the modified authentication information.

5. Method according to any of claims 1 to 3, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising the steps of:

- generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication standard, an authentication response RES;
- modifying, preferably using a one-way function, the authentication parameter RES on the basis the identified communications channel.

6. Method according to any of claims 2-5, the method further comprising the steps of:

- the terminal sending a service request via a predetermined communications channel to the network;
- the network generating an expected service code XSC on the basis of the type of communications channel the service request was sent to the network;
- determining on the basis of expected service code XSC an expected response XRES.

7. Method according to claim 6, the method further comprising the steps of:

- comparing the expected response XRES with the authentication response RES send by the terminal to the network; and,

- determining the terminal to be in an un-trusted state if RES is not equal to XRES.

8. Method according to any of claims 1-7, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

9. Service interface module for use in a terminal, preferably configured to securely process all authentication information transmitted to and from an identity module in the terminal, the service interface module comprising:

- a receiver for receiving an authentication signal from the network via one of the communications interfaces of the terminal;
- a channel identifier for identifying the communication channel through which the authentication signal was received, preferably by providing a service code associated with the identified communication channel;
- a channel interface for establishing a secure communication channel between the module and an identity module of the terminal.

10. Service interface module according to claim 9, the module further comprising:

- a modifier for modifying an authentication response of the identity module on the basis of the identified communication channel, or means for transmitting information regarding the identified communications channel to the identity module, or means for modifying the authentication signal received from the network.

11. An identity module, preferably a smartcard, for establishing a safe communication channel with a service interface module as claimed in claims 9 or 10, the identity module comprising: a calculator for calculating a response RES - preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA

- upon receipt of an authentication request; and, optionally, a modifier for modifying the response RES on the basis of a predetermined mathematical function using information on the identified communication channel.

12. A terminal, preferably a mobile device, for accessing network services, the terminal being configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal.

13. The terminal as recited in claim 12 wherein the terminal is configured to:

- receive an authentication request from the network;
- determine a service code associated with the type of communication channel via which the authentication request was received by the terminal and;
- send in response to the authentication request an authentication response RES to the network wherein the authentication response depends on the determined service code.

14. A network node for service-based authentication of a terminal to a network, the network node being configured to generate in response to the receipt of an authentication data request a modified expected response XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

15. A network node as recited in claim 14 wherein the network node is configured to:

- receive an authentication data request;
- determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and;

- generate in response to the receipt of the authentication data request an expected response XRES, wherein the expected response depends on the determined expected service code.

16. A system for service based authentication to a network, comprising:

- a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal;
- a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

17. A system as recited in claim 16, comprising:

- a terminal configured to receive an authentication request from the network, to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal and to send in response to the authentication request an authentication response RES to the network wherein the authentication response depends on the determined service code and;
- a network node configured to receive an authentication data request, determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and to generate in response to the receipt of the authentication data request an expected response XRES, wherein the expected response depends on the determined expected service code.

18. A computer program product comprising software code portions configured for, when run in the memory of a terminal, preferable a mobile device, executing the method steps according to any of claims 1-5.

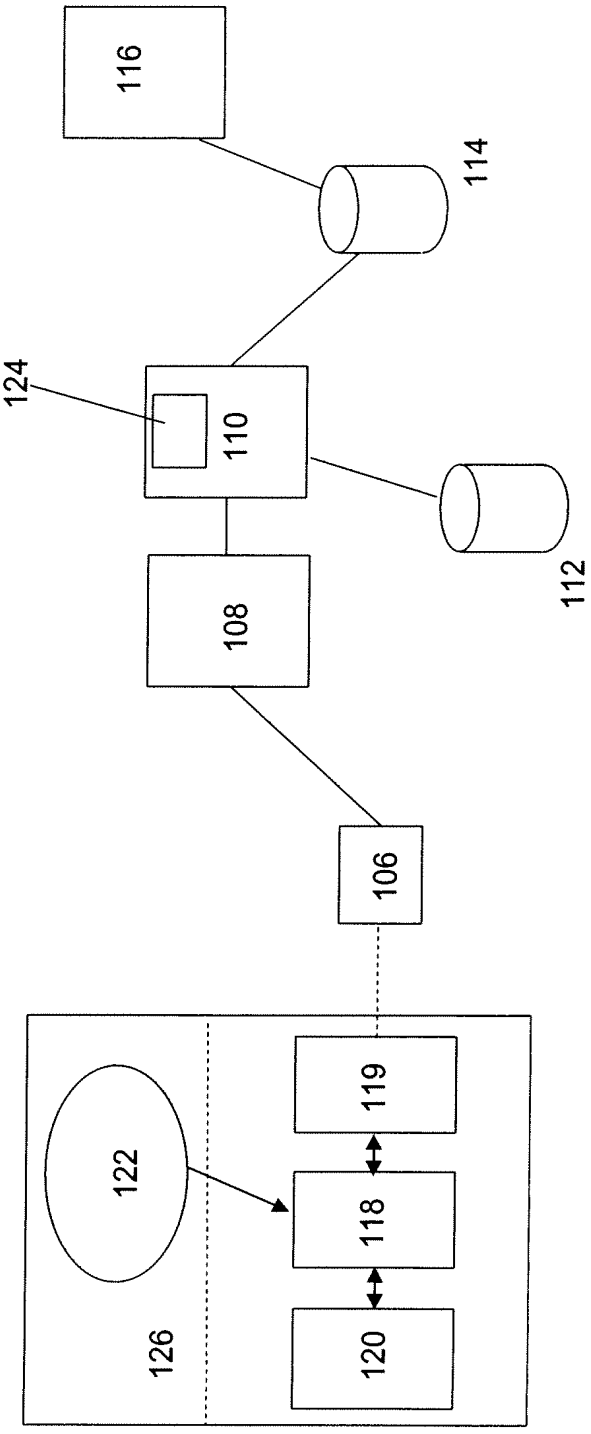


Figure 1

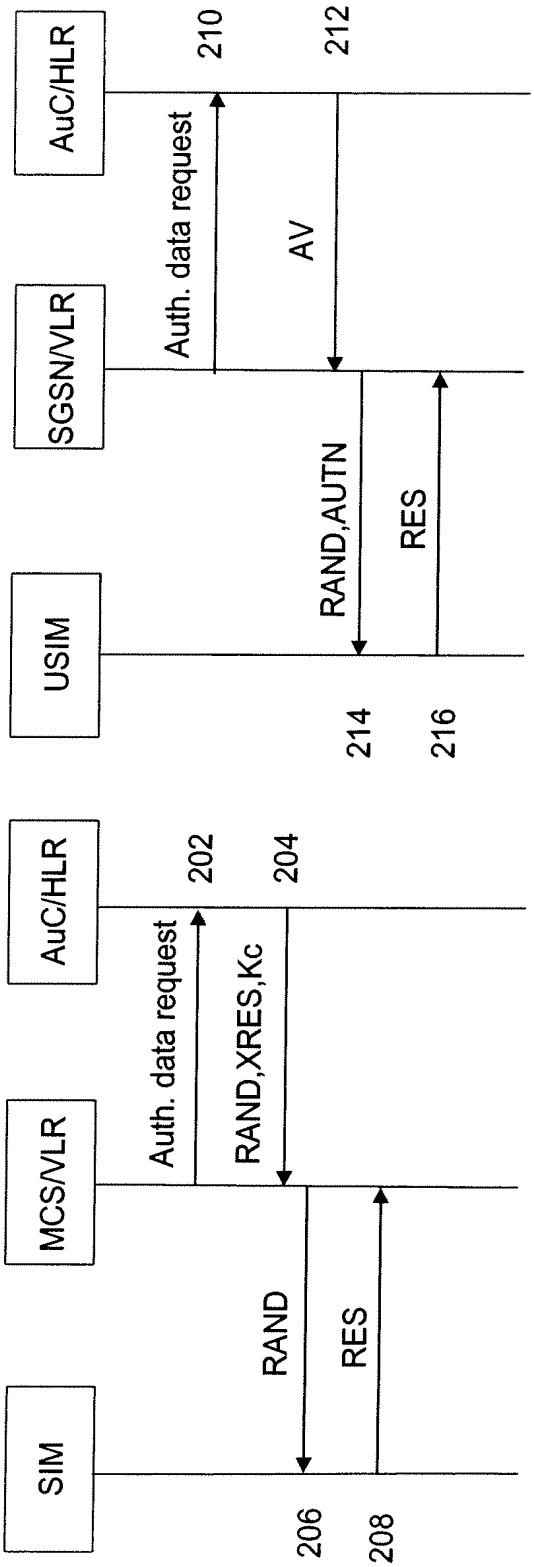

AuC/HLR
SGSN/VLR
USIM
Auth. data request
AV
RAND,AUTN
RES
210
212
214
216
(b)
AuC/HLR
MCS/VLR
SIM
Auth. data request
RAND,XRES,Kc
RAND
RES
202
204
206
208
(a)
200

Figure 2

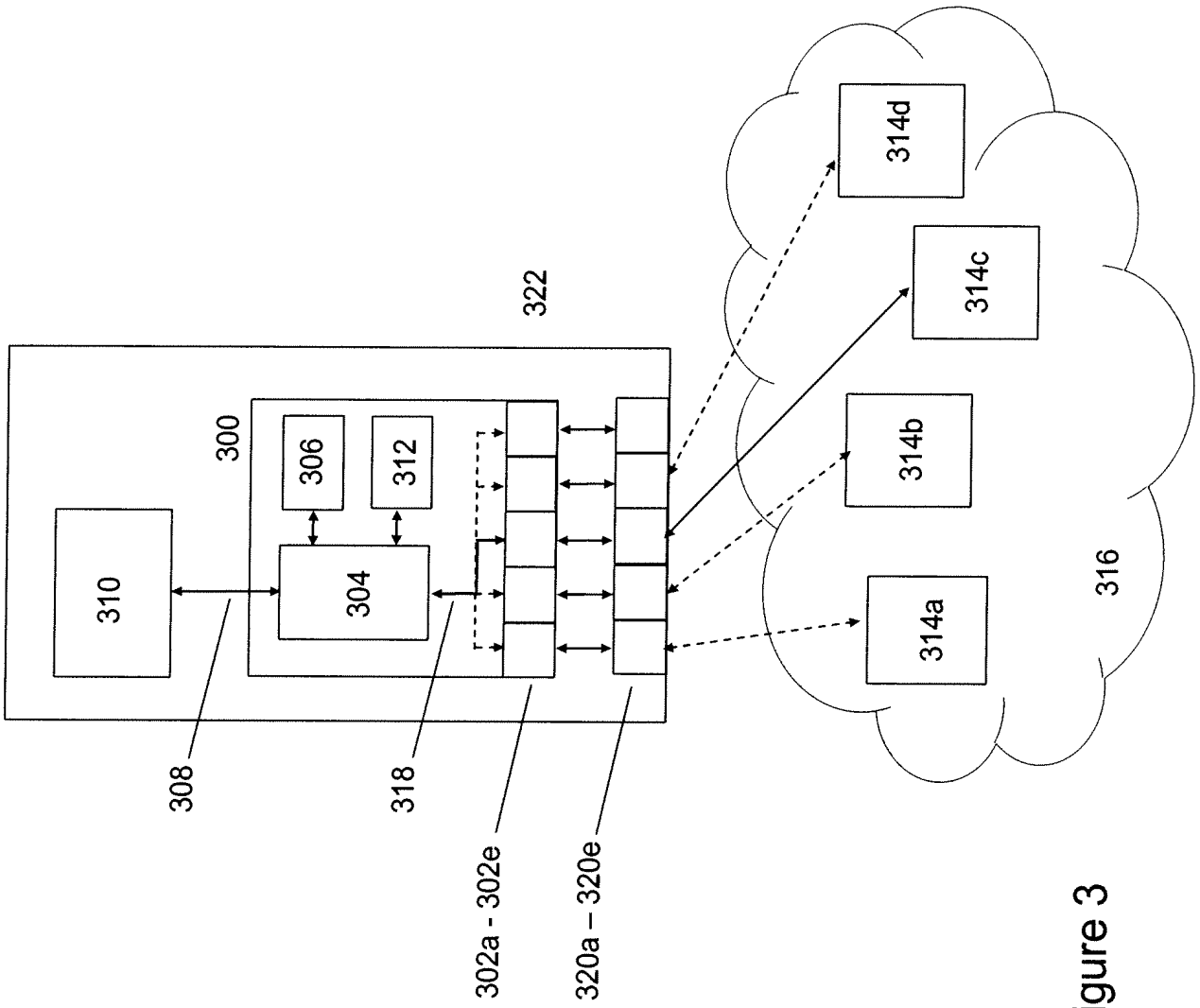

322
300
306
312
310
304
308
318
302a - 302e
320a – 320e
314d
314c
314b
314a
316

Figure 3

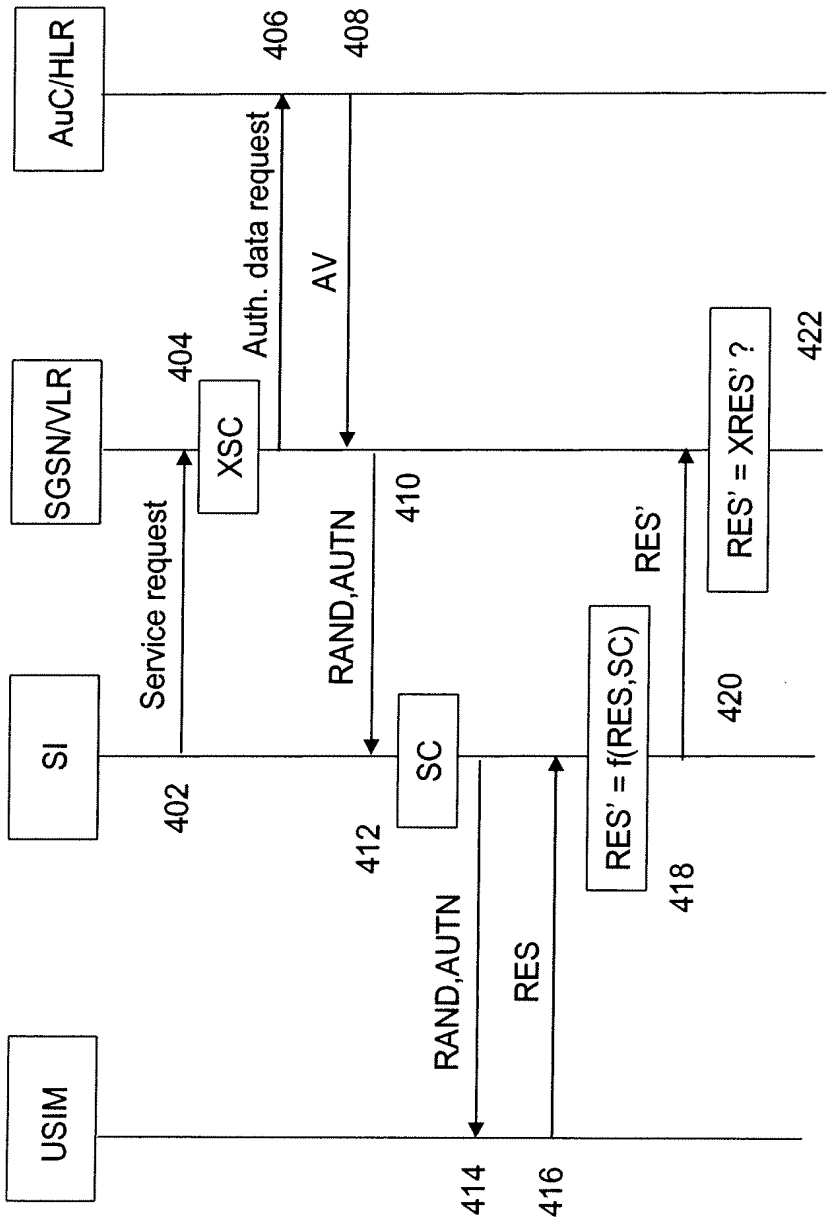

AuC/HLR
SGSN/VLR
SI
USIM
406
408
404
Auth. data request
AV
XSC
Service request
RAND,AUTN
410
SC
402
412
RAND,AUTN
RES
RES' = f(RES,SC)
RES'
420
RES' = XRES' ?
422
418
414
416
400

Figure 4

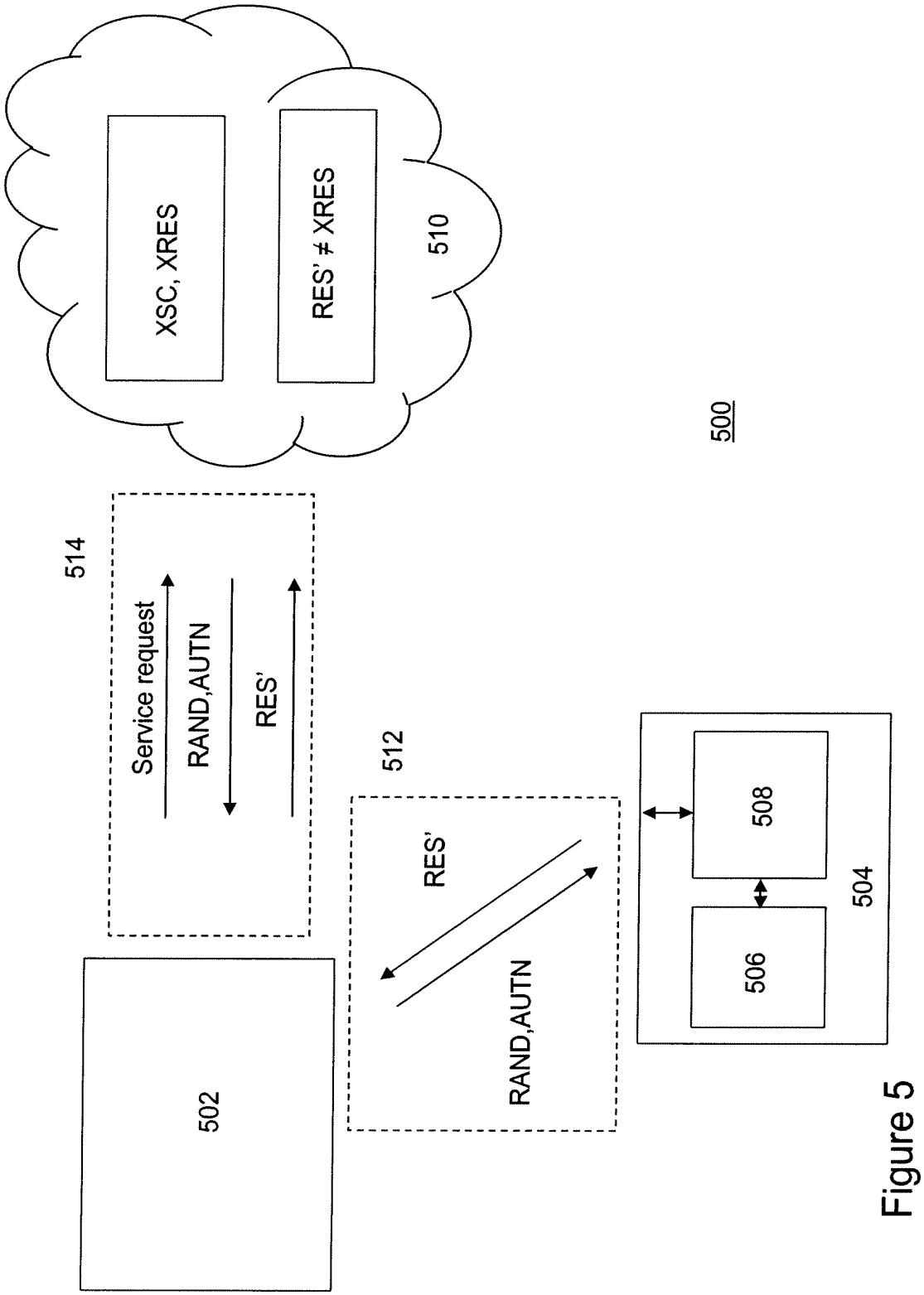

XSC, XRES
RES' ≠ XRES
510
500
514
Service request
RAND,AUTN
RES'
512
RES'
RAND,AUTN
502
508
506
504

Figure 5

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP2009/067201

International filing date: 15 December 2009 (15.12.2009)

Document type: Certified copy of priority document

Document details: Country/Office: EP
Number: 08021705.2
Filing date: 15 December 2008 (15.12.2008)

Date of receipt at the International Bureau: 01 February 2010 (01.02.2010)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung	Certificate	Attestation
Die angehefteten Unterlagen stimmen mit der als ursprünglich eingereicht geltenden Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.	The attached documents are exact copies of the text in which the European patent application described on the following page is deemed to have been filed.	Les documents joints à la présente attestation sont conformes au texte, considéré comme initialement déposé, de la demande de brevet européen qui est spécifiée à la page suivante.

Patentanmeldung Nr.	**Patent application No.**	**Demande de brevet n°**
	08021705.2 / EP08021705	

The organization code and number of your priority application, to be used for filing abroad under the Paris Convention, is EP08021705.

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le President de l'Office européen des brevets
p.o.

R.C. van Dijk

Anmeldung Nr:
Application no.: 08021705.2
Demande no :

Anmeldetag:
Date of filing: 15.12.08
Date de dépôt :

Anmelder / Applicant(s) / Demandeur(s):

Koninklijke KPN N.V.
Maanplein 55
2516 CK The Hague/NL

Nederlandse Organisatie voor Toegepast-
Natuurwetenschappelijk Onderzoek TNO
Schoemakerstraat 97
2628 VK Delft/NL

Bezeichnung der Erfindung / Title of the invention / Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se référer à la description.)

Service-based authentication to a network

In Anspruch genommene Priorität(en) / Priority(Priorities) claimed / Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen / State/Date/File no. / Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation / International Patent Classification / Classification internationale de brevets:

H04L29/06

Am Anmeldetag benannte Vertragstaaten / Contracting States designated at date of filing / Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR

Service-based authentication to a network.

Field of the invention

The invention relates to a service-based authentication to a network and, in particular, though not exclusively, to a method and a system for a service-based authentication of a terminal to a network and a service interface module for use in such system.

Background of the invention

The new generation mobile devices, such as smart phones, provide more and more enhanced computational functionalities via open network connections. Such mobile devices are e.g. capable of receiving e-mail, share software with one another through short-range connections, downloading and executing software from the Internet, making automated calls and act under remote control. Hence, similar to a personal computer, mobile devices and in particular the software components involved in the setting up of a connection between the mobile device to the network, are vulnerable to attacks of malicious code (malware). Typically malware attempts to make misuse of mobile device or to simply disrupt legitimate use of a mobile device.

Typically, malware makes use of security flaws in the authentication procedure which provides a subscriber access to a network. For example the GSM authentication and key agreement (AKA) only authenticates the mobile device to the network, but not the other way around. The GSM AKA is therefore vulnerable to so-called false base station attacks wherein an attacker pretends to be a valid base station. In the UMTS AKA part of these threats are mitigated by using a mutual authentication wherein the mobile device has to authenticate itself to the Visitor Location Register (VLR) and the VLR has to authenticate itself to the mobile device. An overview of the security threats in the GSM AKA and the way a

number of these threats are counteracted by the UMTS AKA are described in ETSI TS 33.900.

From TS 33.900 it follows that the UMTS AKA is still vulnerable to security attacks. For example, the UMTS AKA is vulnerable to the so-called man-in-the-middle attacks, wherein a mobile device of an attacker may use authentication information from the (U)SIM of the victim in order to obtain access to the network. Such a man-in-the-middle attack allows network access as if the connection was set up by the victim. As the network cannot distinguish between a legal situation and such attack the malware allows to set up calls on the expenses of the victim thereby causing substantial damage.

Summary of the invention

It is an object of the invention to reduce or eliminate at least one of the drawbacks known in the prior art and to provide in a first aspect of the invention a method for service-based authentication of a terminal to a network. The terminal comprises one or more communications interfaces for allowing the terminal to setting-up a communication channel with the network. The method comprises the steps of: sending a service request for access to a network service; receiving in response to the service request an authentication request from the network; identifying the communication channel through which the authentication request was received; and, sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

The method allows the network to determine through which communication channel authentication information is transmitted to the network. Determination of the communication channel can be easily achieved by identifying the communication interface through which the authentication request is received. Such service-based authentication method effectively prevents misuse of authentication information, e.g. a man-in-the-middle attack wherein an attacker uses

authentication information from the (U)SIM of the victim in order to obtain access to the network.

Furthermore, the method is compatible with all or at least most existing and proposed AKA's. It only requires determination of the communication channel through which the request was received and secure insertion of information regarding the communication channel into the response.

In one embodiment the method further comprises the steps of: determining a service code associated with the identified communication channel; calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information regarding the identity of the communication channel through which the authentication request was received into the response.

The information regarding the communication channel through which the authentication information is transmitted to the network is securely inserted in the response of the identity module of the terminal. Hence, it is not possible or at least very difficult for malware to detect and/or modify the service channel information.

In another embodiment the terminal used in the method comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.

By using a service interface module as a trusted hardware module in the terminal, a very safe and reliable method is achieved for sending the information regarding the identity of the communication channel to the network. Preferably, the service interface module is configured to receive all incoming authentication signals from the network. Hence, all authentication request will be routed via the service interface module to the identity module of the terminal.

In yet another embodiment the authentication request comprises authentication information, preferably a random

challenge RAND and the method further comprises the steps of: modifying the authentication information on the basis of the identified communications channel; generating, preferably using an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES on the basis of the modified authentication information.

In one embodiment the authentication request comprises authentication information, preferably a random challenge RAND and the method further comprises the steps of: generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES; modifying, preferably using a one-way function, the authentication parameter RES on the basis the identified communications channel.

This embodiment allows simple and safe implementation of the method by using a service interface module which securely communicates with the identity module. Identification of the communication channel and secure insertion of the information regarding the identified communication channel may take place in the service interface module so that no modifications of the identity module are required. This implementation is thus compatible with existing identity modules.

In another embodiment the method further comprises the steps of: the terminal sending a service request via a predetermined communications channel to the network; the network generating an expected service code XSC on the basis of the type of communications channel the service request was sent to the network; determining on the basis of expected service code XSC an expected response XRES.

In one embodiment the method further comprises the steps of: comparing the expected response XRES with the authentication response RES send by the terminal to the network; and, determining the terminal to be in an un-trusted state if RES is not equal to XRES.

Hence, the method only requires a simple modification in the existing network in the sense that it requires a network node which is configured to identify the communication channel through which the service request is received by the network and to extract the information regarding the communication channel encrypted in the terminal response.

In one embodiment the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

In a further aspect the invention relates to a service interface module for use in a terminal, preferably configured to securely process all authentication information transmitted to and from an identity module in the terminal, wherein the service interface module comprises: a receiver for receiving an authentication signal from the network via one of the communications interfaces of the terminal; a channel identifier for identifying the communication channel through which the authentication signal was received, preferably by providing a service code associated with the identified communication channel; an interface for establishing a secure communication channel between the module and an identity module of the terminal.

All functionality required in the terminal for implementation of the method can be simply located in one trusted hardware module which securely communicates with the identity module.

In one embodiment the service interface module further comprises a modifier for modifying an authentication response of the identity module on the basis of the identified communication channel, or sender for transmitting information regarding the identified communications channel to the identity module, or modifier for modifying the authentication request received from the network.

In another aspect the invention relates to an identity module, preferably a smartcard, for establishing a safe communication channel with a service interface module as described above. The safe communication channel may for

example consist of a link protected with cryptography or a direct hardware link between the service interface module and the identity module that cannot be interfered with by an attacker. The identity module comprises: a calculator for calculating a response RES - preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA - upon receipt of an authentication request; and, optionally, a modifier for modifying the response RES on the basis of a predetermined mathematical function using information on the identified communication channel.

In yet another aspect the invention relates to a terminal, preferably a mobile device, for accessing network services, wherein the terminal is configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal.

In one embodiment the terminal comprises a service interface module according as described and, optionally, an identity module as described above.

In a further aspect the invention relates to a network node for service-based authentication of a terminal to a network, wherein the network node is configured to generate in response to the receipt of an authentication data request a modified expected response XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

In one embodiment the network node comprises: a receiver for receiving a service request from a terminal; a generator for generating an expected service code XSC on the basis of the type of communication channel the service request was sent to the network; a generator for generating an expected response XRES or a receiver for receiving from another network node an expected response XRES, preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA; and, a modifier the expected response XRES on the basis of a predetermined mathematical function, preferably a one-way

function, using the expected service code XSC as an input parameter.

In one embodiment the network node further comprises: a receiver for receiving a response RES from a terminal; a comparator for comparing the response RES with the modified expected response XRES'.

In yet a further aspect the invention relates to a system for service based authentication to a network, comprising: a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal; and, a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

The invention also relates to a computer program product comprising software code portions configured for, when run in the memory of a terminal, preferable a mobile device, executing the method steps as described above.

The invention will be further illustrated with reference to the attached drawings, which schematically will show embodiments according to the invention. It will be understood that the invention is not in any way restricted to these specific embodiments.

Brief description of the drawings

Fig. 1 depicts a schematic representation of a system according to one embodiment of the invention.

Fig. 2 illustrates a schematic flow diagram of the GSM authentication procedure and the UMTS authentication procedure.

Fig. 3 depicts the service interface module according to one embodiment of the invention.

Fig. 4 depicts a flow diagram according to one embodiment of the invention.

Fig. 5 illustrates prevention of a fraudulous authentication procedure by using the invention.

Detailed description

Fig. 1 illustrates a schematic representation of a communications system **100** according to one embodiment of the invention. The system comprises a terminal **102** connected to a communications network **104**. In one embodiment the network may be a 2G-type (e.g. GSM) mobile network comprising a base transceiver station (BTS) **106** serving as an access node. The BSC is connected via a base station controller (BSC) **108** to a mobile switching center (MSC) **110** of e.g. a visiting network (VN). The MSC is linked to a visited location register (VLR) **112**, which is a database that stores user related data and performs security functions. The MSC is further linked to a home location register (HLR) **114** which is located in the home network (HN) where the user of the terminal **102** has a subscription with the network operator. The HLR **114** stores user related data, e.g. subscription related data, and co-operates with the MSC/VLR **110** to keep track of the location of the terminal. The HLR is connected to an authentication centre (AuC) **116**. The authentication centre (AuC) comprises (amongst others) algorithms for the calculation of authentication parameters used in the authentication procedure. For each subscriber the AuC stores a secret authentication key K which is also stored in an associated identity module, e.g. a (U)SIM card or the like, located in the terminal.

Alternatively, the network in Fig. **1** may also depict a 3G-type (e.g. UMTS) mobile network comprising 3G network elements. In that case, the network may comprise a radio base station (Node-B) **106** connected via a Radio Network Controller (RNC) **108** to a Serving GPRS Support Node (SGSN) **110**. The SGSN is further connected to a VLR **112** and an AuC/HLR **114,116** in a similar way as in the 2G-type network as described above.

In a further embodiment the communications network **104** may comprise IMS-based network elements in the form of a set of Call/Session Control Functions (CSCF) such as a Proxy-CSCF (P-CSCF), an Interrogating-CSCF (I-CSCF), a Serving-CSCF (S-CSCF) and a Home Subscriber Server (HSS). In yet further embodiments the communications network may comprise 3GPP LTE or 3GPP SAE network elements.

The terminal **102** may be a personal computer or a mobile device such as a smart phone, a personal digital assistant (PDA), a laptop or any other mobile communications device capable of providing services over one or more networks. The terminal comprises a service interface (SI) module **118**, an operating system (OS) **126** and an identity module **120**.

The SI module **118** acts as a central access point to wired and wireless network services and comprises for that purpose a number of service interfaces. For example, for wireless services, it includes an interface to an RF module, e.g. a 2G or 3G radio card, comprising an RF receiver connecting to one more antennas. **Fig. 1** depicts an exemplary implementation wherein a radio card module **119** provides radio contact with the base station **106**. The RF interface of the radio card is capable of receiving and/or transmitting RF signals in accordance with various wireless technologies using licensed frequency bands (e.g. TDMA for GSM services or W-CDMA for UMTS services). The radio card must have a secure interface to the SI module. Beside the interface to the RF module the SI module may comprise a number of interfaces to other wireless interface modules, e.g. wireless interface modules using non-licensed frequency bands such as the IEEE 802.11 interface for WLAN services, the IEEE 802.15.1 interface for Bluetooth services, an DECT interface as described in ETS 300 175, etc.

The SI module may also comprise interfaces to one or more wired interface modules, e.g. an Ethernet interface allowing the SI module to be connected to the network using a wired Ethernet communication channel. An access and configuration (AC) manager in the SI module manages the set-up

of a communication channel to an access node of a network or - in case of a short-range connection such as Bluetooth - to another terminal. It determines the correct parameter for operation under a specific wired or wireless technology and/or protocol associated with the networks services requested by the terminal. Further, the SI module is configured to securely include information regarding the used interface in the data sent to a Service Identification Unit (SIU) **124** in the network. The interaction between the SI module **118** and the SIU **124** is explained hereunder in more detail.

The Operating System (OS) of the terminal comprises a kernel which manages the resources of the mobile device e.g. the Central Processing Unit (CPU), memory for storing program instructions and data and Input/Output (I/O) devices such as the radio module. Further, the OS comprises Application Programming Interfaces (APIs) through which application programs **122** may access services offered by the OS. The OS may comprise APIs for setting up wired or wireless connections via one of the interfaces modules.

The identity module **120**, which is typically removable, may be a UICC (Universal Integrated Circuit Card) for use in mobile devices suitable for 2G-type network services (GSM) or 3G-type network services, (UMTS). To that end, the UICC may comprise a Subscriber Identity Module (SIM) application comprising SIM functions and/or a UMTS Subscriber Identity Module (USIM) application comprising USIM functions. It is to be understood that the identity module is not limited to SIM and/or USIM applications. In further embodiments, the identity module may be an IP Multimedia Sub-system SIM (ISIM) for authenticating and accessing IMS-based services according to a predetermined IMS-based AKA as e.g. described in ETSI technical specification TS 33.203 or an extensible authentication protocol (EAP) based SIM for authentication and accessing a network according to a predetermined EAP-based AKA as described for instance in RFC4187.

The identity module may comprise a processor, one or more memory components e.g. ROM, RAM and/or EEPROM and I/O circuitry. For authentication purposes the UICC comprises a

secret service-subscriber authentication key K and one or more algorithms for calculating a response comprising one or more authentication parameters upon the reception of a random challenge.

Fig. 2(a) illustrates a schematic flow diagram of the standard GSM authentication procedure which may be used by the SIM module in the identity module. In the GSM standard the MSC initiates, in response to a service request of a network service originating from the terminal, a request for authentication data to the AuC/HLR (step **202**). A random number generator at the AuC/HLR generates a random value RAND that is input to the GSM A3/A8 algorithms which generate an expected response XRES and a cipher key K_C. The triplet {RAND, XRES, K_C} is returned to the MSC (step **204**) that subsequently forwards the RAND value to the SIM card of the terminal (step **206**). Corresponding calculations are performed by the terminal, typically by the integrity module, which returns a calculated response RES back to the MSC (step **208**). By comparison of the RES with the XRES the MSC can authenticate the terminal to the network.

In the standard UMTS authentication procedure similar steps as the GSM procedure are performed. However, in order to improve the security additional parameters and a set of eight functions f0-f5,f1*,f2* are used. **Fig. 2(b)** illustrates a schematic flow diagram of the UMTS authentication procedure, which may be used with a USIM application in the identity module. In response to a request for authentication data from the SGSN/VLR (step **210**), the AuC/HRL generates a random number RAND (using function f0) and a fresh sequence number SQN. The AuC/HRL provides the secret authentication key K (which is both stored in the AuC and the USIM but never directly exchanged) and an operator specific Authentication Management Field AMF. These four parameters are fed into the five symmetric encryption functions f1-f5, resulting in five new parameters: the Message Authentication Code (MAC), the Expected Response (XRES), the Ciphering Key (CK), the Integrity Key (IK) and the Anonymity Key (AK). The sequence number SQN is separately encrypted into SQN^1.

The AuC/HLR returns these parameters in an authentication vector (AV) {AUTN,RAND,XRES,CK,IK} to the SGSN/VLR (step **212**) wherein the Authentication token AUTN is a triplet {SQN^1,AMF,MAC}. Thereafter, the SGSN/VLR forwards an Authentication and Ciphering request comprising RAND and AUTN to the mobile device (step **214**). Using RAND and AUTN the USIM calculates - amongst others - a response RES, which is sent back to the SGSN (step **216**) and compared with the XRES as received from the AuC/HLR.

The keys for ciphering and integrity checking have a limited lifetime to prevent attempts to break the cipher or integrity protection by brute force long duration monitoring attacks. Upon expiry, a new set of ciphering and integrity keys are generated with a re-authentication between the terminal and the network. This re-authentication process is regularly repeated.

The GSM AKA is described in detail in ETSI standards GSM 02.09 and GSM 03.20 and the UMTS AKA described in detail in ETSI technical specification TS 33.102, which are hereby incorporated by reference.

Fig. 3 depicts an SI module according to a preferred embodiment of the invention The SI module **300** is located in a terminal **322** and comprises a number of interfaces **302a-302e**, which are connected, preferably through one or more secure communication channels , to associated interface modules **320a-320e**. The interface modules are located in the terminal and used for setting up a network connection with the network **316**. The SI module is configured to generate a service code (SC) identifying the specific service interface used to set up a wired or a wireless communication channel. To that end, the AC manager **304** in the SI module may use a look-up table **306** comprising the different types of service interfaces supported by the mobile terminal and the associated service codes. The AC manager may be implemented in the form of a processor and one or more memory modules comprising e.g. the configuration data of the look-up table.

The hardware of the terminal is preferably configured in such a way that all incoming authentication requests for a

network service received by one of the interfaces **302a-302e** will be centrally routed via the SI module to the UICC connected to the SI module. Such hardware architecture ensures that all incoming authentication requests are identified with respect to the communication channel the request was received by the terminal. Further, the SI module is configured to provide a secure communication channel **308** with the UICC **310** connected to the SI module. Hence, preferably, the SI module is implemented in the form of one or more trusted hardware components.

If, for example, the terminal **322** receives a network signal, e.g. a 3G signal, via a 3G RF interface module **320c** and the 3G interface **302c** of the SI module, the signal is translated into a digital signal in accordance with the technical specifications of the wireless air interface. Thereafter the digital signal comprising the authentication request is transmitted via the SI module to the UICC **310**. Further, the AC manager **304** identifies the service code associated with the 3G RF interface **302c** using a look-up table **306**. The service code is used by the SI module to provide the network with information regarding the origin of the authentication request.

The UICC processes the authentication request according to an AKA of a telecommunications standard, e.g. a GSM AKA or a UMTS AKA as described in relation with **Fig. 2** and then returns a response RES back to the SI module. Thereafter, the SI module uses a predetermined mathematical algorithm f stored in a secure memory **312** of the SI module in order to securely include the information embodied in the service code into the response RES received from the UICC. Preferably, the mathematical algorithm f is a so-called one-way function which is easy to compute but impossible or very hard to invert. A suitable one-way function may be a secure hash operation with the SC. Inserting the service code into the response allows the SI module to inform the network **316** about the communication channel (Bluetooth **314a**, WLAN **314b**, 3G **314c**, Ethernet **314d**, etc.) through which the authentication request

was received from the network in a way which is not, or at least very difficult, to modify by malware.

In order for the network to extract the channel information, the network, preferably the SGSN/VLR or an equivalent network node such as the MCS/VLR, comprises an Service Identification Unit (SIU). The SIU comprises a function f which is identical to the function f used by the SI module. Further, the SIU is configured to determine through what type of communication channel a service request is received.

The advantage of the architecture of the SI module as depicted in **Fig. 3** is that the specifications of the (U)SIM do not require changes. The implementation is simple and only requires the installation of a SI module in the terminal and a SIU in the network. Moreover, the architecture is backwards compatible with conventional equipment, i.e. terminals and network nodes (e.g. SGSN/VLR or MCS/VLR) which do not comprise a SI mode or a SIU.

A more detailed explanation on the functioning of the SIU will be given in relation to **Fig. 4**.

Fig. 4 depicts a process flow **400** between a UMTS network and a terminal comprising a USIM and an SI module as described in relation with **Fig. 1** and **3**. The process is started by a terminal application requesting a UMTS service from the network. The request triggers the RF interface module to set-up up a wireless UMTS communication channel between the terminal and an access node of the requested UMTS network. Thereafter, a service request is transmitted via the wireless communication channel to the SGSN/VLR (step **402**).

Then the SIU in the SGSN/VLR determines through which service interface (UMTS, GSM, WiFi, Bluethooth, etc.) contact was established with the terminal. On the basis of the identified service interface information an expected service code XSC is determined (step **404**). The SIU may determine XSC by retrieving the service code associated with the identified service interface (in this case a UMTS service) from a look-up table - substantially identical to the one used by the SI

module in the terminal - stored in a secure memory of the SI module.

In response to the service request, the SGSN/VLR sends an authentication data request to the AuC/HLR of the network (step **406**). The AuC/HLR generates a UMTS authentication vector AV, which is sent back to the SGSN/VLR (step **408**). Subsequently RAND and AUTN are sent in an Authentication and Ciphering request via the wireless communication channel to the terminal (step **410**). When the RF interface module of the terminal receives the radio signal comprising the request, the signal is converted to a digital signal. The AC manager identifies the service code associated with the interface used by the SI module to communicate with the RF module (step **412**). Thereafter, the digital signal comprising the RAND and AUTN is forwarded to the USIM (step **414**), which calculates the response RES using e.g. the f1-f5 algorithms of the UMTS AKA. Then the USIM sends the response RES back to the SI module (step **416**).

Using the SC and the one-way function f, the SI determines a modified response RES'=f(RES,SC) (step **418**), hence securely inserting information about the communication channel through which the request was received. This way, the response RES' becomes specific for the service it is meant for. The response RES' is subsequently transmitted back via RF interface to the SGSN/VLR in the network (step **420**) for comparison with an expected response XRES' (step **422**). The expected response XRES' may be determined by the SIU using the one-way function f with the expected response XRES determined on the basis of the UMTS AKA and the SC as the input parameters: XRES'=f(XRES,SC).

Thereafter a comparison between the terminal response RES' and the expected response XRES' is made. If RES' is equal to XRES' then this provides an indication for the network that the terminal received an authentication request via the communication channel that was expected by the network. In that case access to the network is granted.

If RES' is not equal to XRES' then an indication to the network is provided that the terminal received an

authentication request via a communication channel different from the communication channel expected by the network. This may provide the network with an indication that the terminal may be corrupted by malware.

It is noted that the invention is not limited to the embodiment as described in relation with **Fig. 3** and **4**. In a further embodiment the UICC (instead of the SI module) comprises the one-way function f for securely inserting the service code information into the response.

After the AC manager has selected the correct SC, the code is inserted into the digital signal comprising the request and send to the identity module for further processing (e.g. authentication and/or computation of the decryption key). Hence, in this variant the digital signal sent by the SI module to the identity module comprises information via which service interface (and hence via which communications channel) the signal was received. Further variants for sending the service code to the identity module may include, e.g. sending the service code to the identity module in a separate signal.

In one embodiment the (U)SIM may modify the authentication information in the authentication request, e.g. a random challenge RAND, on the basis of the service code SC and subsequently calculate a response RES on the basis of an authentication and key agreement (AKA) of a telecommunications standard. For example, in the case of a GSM service the SIM may perform the steps: $RAND'=f(RAND,SC)$ and $RES'=A3(RAND',K_C)$. In another variant, the SIM first calculates the response RES on the basis of the RAND and then modifies RES on the basis of SC: $RES=A3(RAND,K_C)$ and $RES'=f(RES,SC)$. In the case of an UMTS service, the f1-f5 algorithms of the UMTS AKA are used instead of the A3 algorithm of the GSM AKA.

Depending on the specific scheme implemented in the USIM, the SIU which comprises the mathematical function f used by the USIM in the terminal, may determine $RAND'=f(RAND, XSC)$ and send this value to the AuC/HLR for determining the expected response XRES' on the basis the UMTS AKA using RAND' as one of the input parameters. Alternatively, the AuC/HRL may first determine XRES on the basis the UMTS AKA using RAND as

one of the input parameters and then send this value to the SIU for determining the expected response XRES'=f(XRES,XSC).

Fig. 5 represents a simplified schematic illustrating how a fraudulous authentication procedure may be prevented using the invention. In this scheme a first terminal **502** of an attacker remotely connects to an infected second terminal **504** of a victim and subsequently requests and uses authentication information from the (U)SIM **506** of the victim to obtain access to the network **510**.

The malware in the second terminal **504** allows the terminal of an attacker **502** to make a first communication channel **512**, e.g. a Bluetooth connection, with the infected terminal of the victim. Other types of connections such as a WiFi connection or a wired connection, such as an Ethernet connection, may also be possible. After connecting to the victim, the attacker starts an authentication procedure to the network by sending a service request via a second communication channel **514** to the AuC/HRL. In response, the attacker will receive an authentication request comprising - amongst others - RAND and AUTN. Instead of responding to the request, the attacker forwards the request to the victim using the Bluetooth connection to the (U)SIM of the victim .

A conventional (U)SIM cannot distinguish between requests originating from different communication channels (e.g. UMTS, GSM, WiFi, Bluetooth, etc.). In that case, the (U)SIM responds to the request by calculating a correct response RES, which is subsequently send via the Bluetooth connection (i.e. the communication connection where the request came from) to the network. The attacker may use this RES to authenticate itself successfully to the network. Using this mechanism the attacker is capable of correctly answering each subsequent Authentication and Ciphering Request from the network.

If however the network **510** and the infected terminal **504** in **Fig.5** are configured as a communications system according to the invention as described in relation with **Fig.1**, the SI module **508** is able to make a distinction between requests originating from different sources. In that case, the

network **510** will determine an expected service code XSC on the basis of the request of the attacker. As the attacker requested a UMTS service via second communication channel **514**, the network will set the XSC to the service code corresponding to a UMTS service. Similarly, the SI module **508** of the infected terminal will modify the RES using the service code corresponding to a Bluetooth communications channel **512**. This modified RES' is sent via the Bluetooth connection to the network, which will then determine that the XRES' calculated by the network on the basis of XSC does not match RES' because the communication channel used to send a request for a UMTS service to the network is different from the communication channel through which the terminal received the authentication request. In that case, the network may take appropriate action.

In one embodiment, the network may calculate the expected response values (XRES'', XRES''', etc.) for each service code available in the look-up table located in a service node of the network. If a XRES' value associated with a particular service code matches RES' then the source of the request received by the terminal may be determined.

This information may be used by the network to take appropriate action. It may e.g. provide no or limited access to the network or place the mobile device in a separate isolation or quarantine network in order to provide remediation services to the mobile device of the subscriber. If the response RES' is neither equal to XRES' nor to the other expected responses then the authentication procedure has failed.

It is to be understood that the invention may also be used with the IMS AKA (3GPP TS 33.203), in Generic Bootstrapping (GBA) applications (see 3GPP TS 33.220, 33.222, 33.223) or with the EAP AKA and/or EAP SIM in WLAN interworking applications. It can also be used in generic access solutions to the mobile network (see 3GPP TS 43.318).

Further, it is to be understood that any feature described in relation to any one embodiment may be used alone, or in combination with other features described, and may also

be used in combination with one or more features of any other of the embodiments, or any combination of any other of the embodiments. Furthermore, equivalents and modifications not described above may also be employed without departing from the scope of the invention, which is defined in the accompanying claims.

CLAIMS

1. Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising the steps of:
- sending a service request for access to a network service;
- receiving in response to the service request an authentication request from the network;
- identifying the communication channel through which the authentication request was received; and,
- sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

2. Method according to claim 1, the method further comprising the steps of:
- determining a service code associated with the identified communication channel;
- calculating the response RES on the basis of the information in the authentication request and the service code, thereby securely including, preferably cryptographically, information regarding the identity of the communication channel through which the authentication request was received into the response.

3. Method according to claims 1 or 2, wherein the terminal comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module, configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.

4. Method according to any of claims 1 to 3, wherein the authentication request comprises authentication

information, preferably a random challenge RAND, the method further comprising the steps of:

- modifying the authentication information on the basis of the identified communications channel;
- generating, preferably using an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES on the basis of the modified authentication information.

5. Method according to any of claims 1 to 3, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising the steps of:

- generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES;
- modifying, preferably using a one-way function, the authentication parameter RES on the basis the identified communications channel;

6. Method according to any of claims 2-5, the method further comprising the steps of:

- the terminal sending a service request via a predetermined communications channel to the network;
- the network generating an expected service code XSC on the basis of the type of communications channel the service request was sent to the network;
- determining on the basis of expected service code XSC an expected response XRES;

7. Method according to claim 6, the method further comprising the steps of:

- comparing the expected response XRES with the authentication response RES send by the terminal to the network; and,

- determining the terminal to be in an un-trusted state if RES is not equal to XRES.

8. Method according to any of claims 1-7, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

9. Service interface module for use in a terminal, preferably configured to securely process all authentication information transmitted to and from an identity module in the terminal, the service interface module comprising:

- a receiver for receiving an authentication signal from the network via one of the communications interfaces of the terminal;
- a channel identifier for identifying the communication channel through which the authentication signal was received, preferably by providing a service code associated with the identified communication channel;
- a channel interface for establishing a secure communication channel between the module and an identity module of the terminal.

10. Service interface module according to claim 9, the module further comprising:

- a modifier for modifying an authentication response of the identity module on the basis of the identified communication channel, or means for transmitting information regarding the identified communications channel to the identity module, or means for modifying the authentication signal received from the network.

11. An identity module, preferably a smartcard, for establishing a safe communication channel with a service interface module as claimed in claims 9 or 10, the identity module comprising: a calculator for calculating a response RES - preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA

- upon receipt of an authentication request; and, optionally, a modifier for modifying the response RES on the basis of a predetermined mathematical function using information on the identified communication channel.

12. A terminal, preferably a mobile device, for accessing network services, the terminal being configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal.

13. A network node for service-based authentication of a terminal to a network, the network node being configured to generate in response to the receipt of an authentication data request a modified expected response XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

14. A system for service based authentication to a network, comprising:

- a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal;
- a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

15. A computer program product comprising software code portions configured for, when run in the memory of a

terminal, preferable a mobile device, executing the method steps according to any of claims 1-5.

ABSTRACT

A method and a system for service-based authentication of a terminal to a network is described, wherein the terminal comprises a number of communications interfaces, each communications interface allowing the terminal to set-up a predetermined communication channel with the network. The method comprises the steps of: sending a service request for access to a network service; receiving in response to the service request an authentication request from the network; identifying the communication channel through which the authentication request was received; and, sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

+ Fig. 1

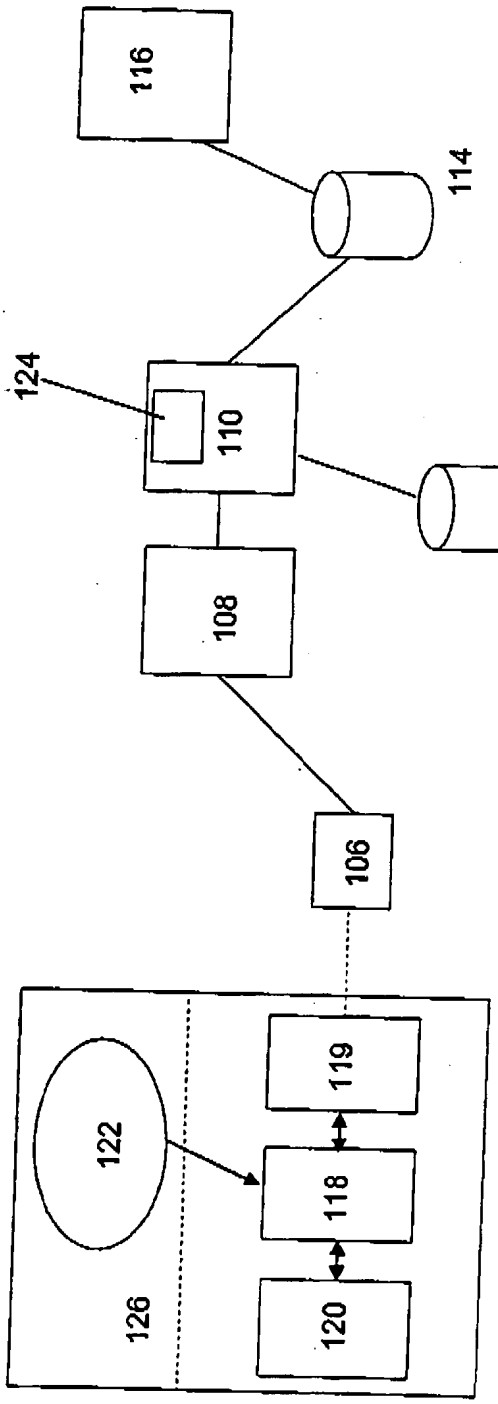


Figure 1

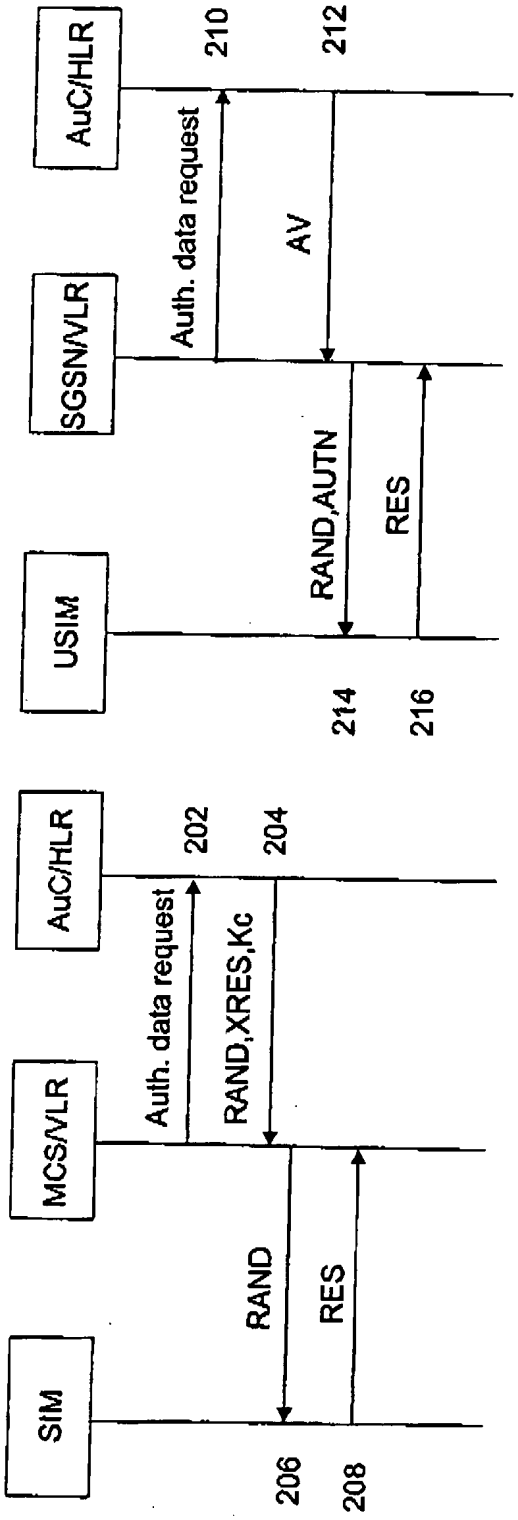

AuC/HLR
SGSN/VLR
USIM
Auth. data request
AV
RAND,AUTN
RES
210
212
214
216
(b)
AuC/HLR
MCS/VLR
SIM
Auth. data request
RAND,XRES,Kc
RAND
RES
202
204
206
208
(a)
200

Figure 2

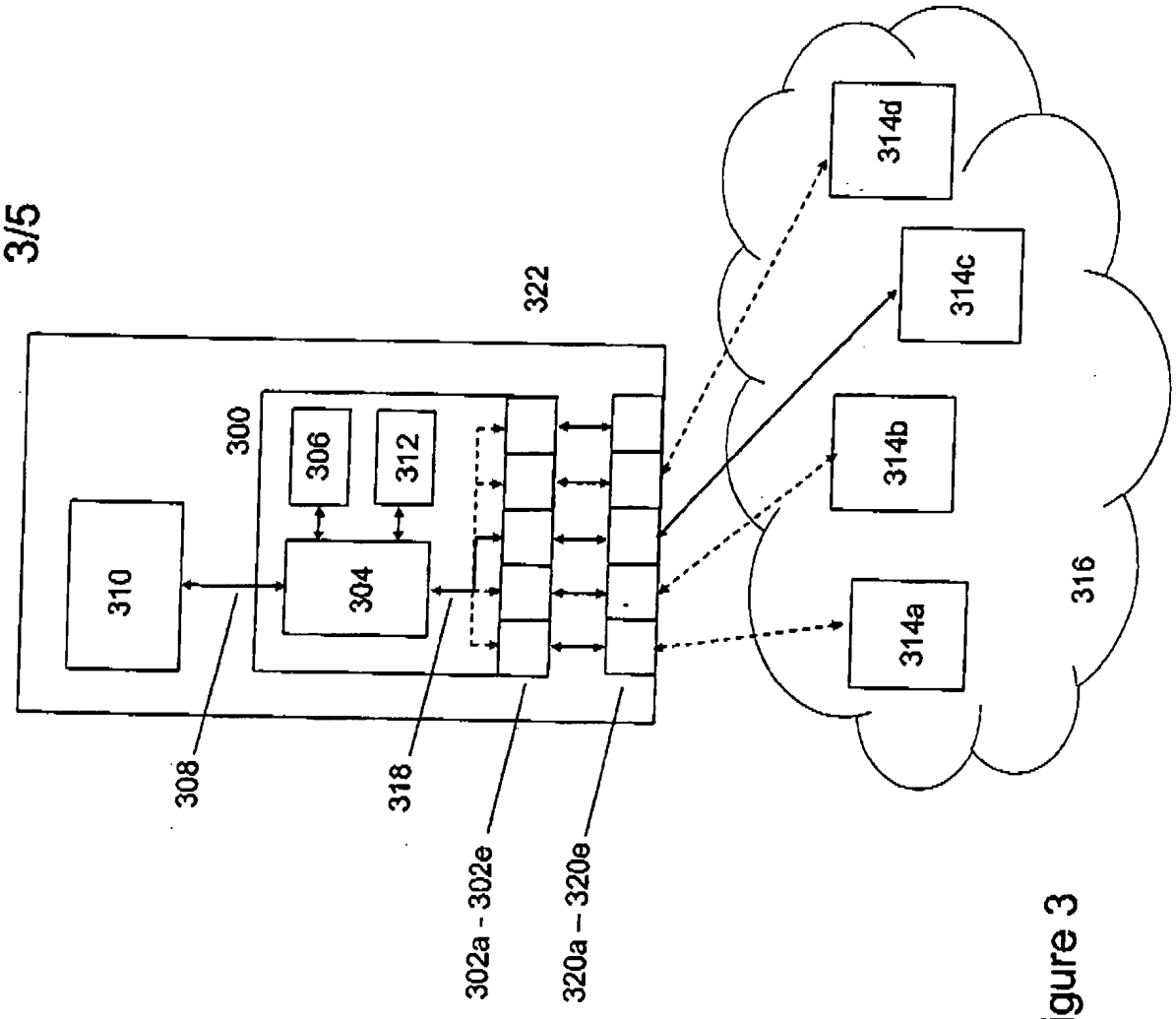

322
300
306
312
310
304
308
318
302a - 302e
320a – 320e
314d
314c
314b
314a
316

Figure 3

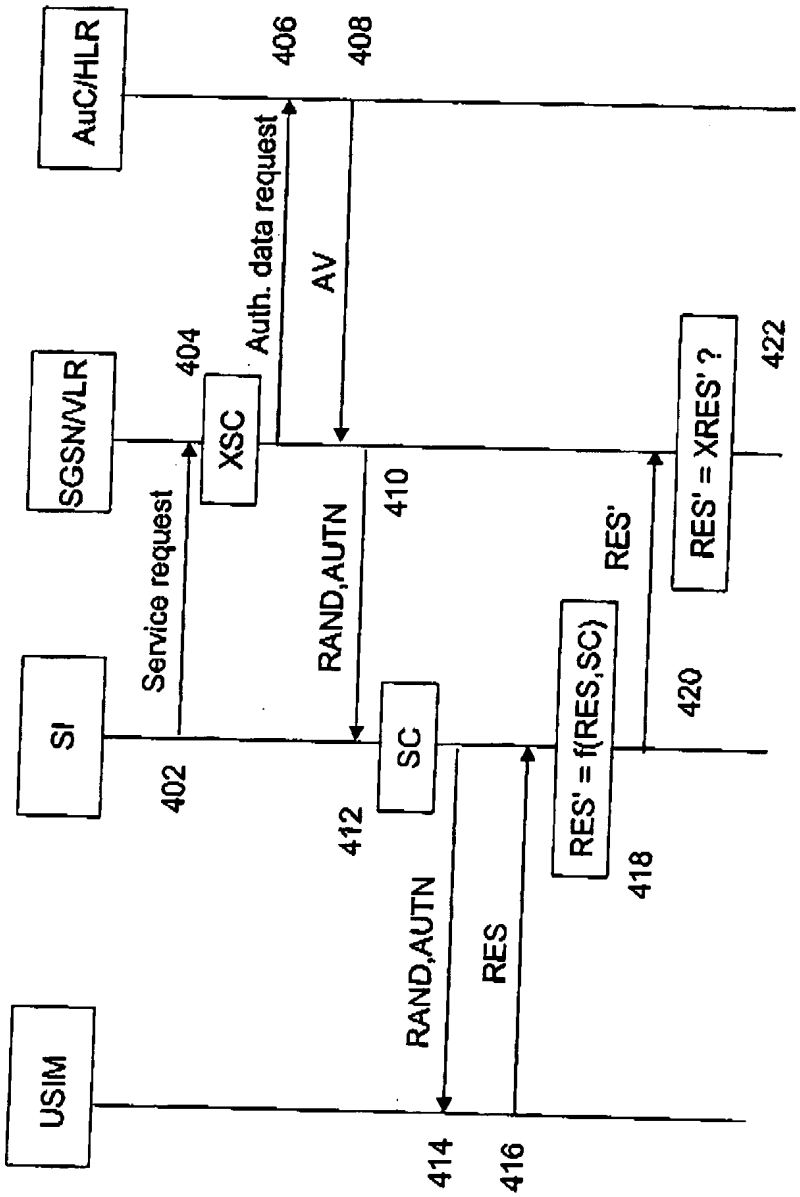

AuC/HLR
406
408
Auth. data request
AV
SGSN/VLR
404
XSC
RES' = XRES' ?
422
Service request
RAND,AUTN
410
RES'
SI
402
SC
RES' = f(RES,SC)
420
412
418
RAND,AUTN
RES
USIM
414
416
400

Figure 4

4/5

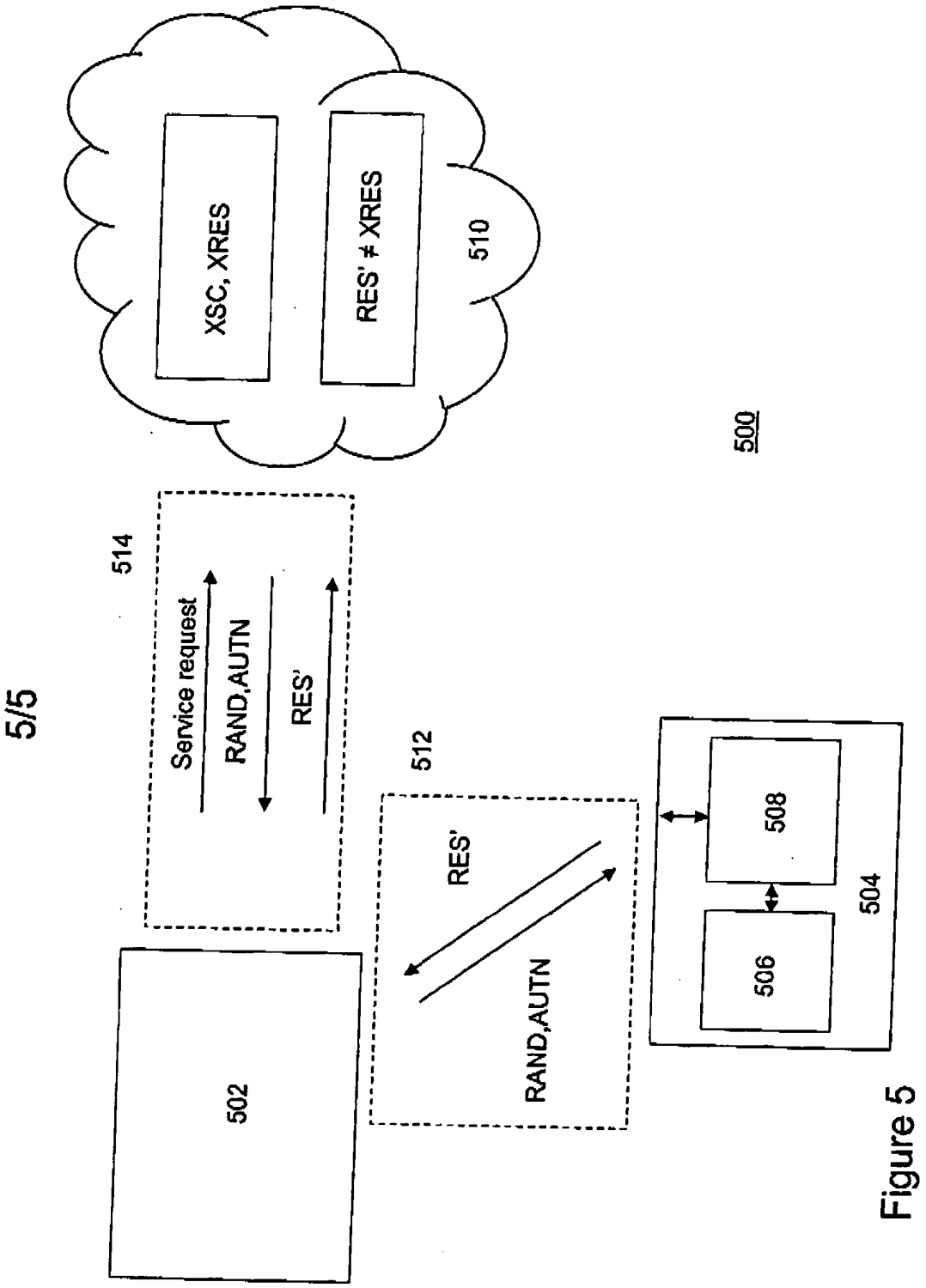


Figure 5

Received at the EPO on Dec 15, 2008 10:29:29. Page 41 of 41

VIII-4-1	**Declaration: Inventorship (only for the purposes of the designation of the United States of America)** Declaration of Inventorship (Rules 4.17(iv) and 51bis.1(a)(iv)) for the purposes of the designation of the United States of America:	I hereby declare that I believe I am the original, first and sole (if only one inventor is listed below) or joint (if more than one inventor is listed below) inventor of the subject matter which is claimed and for which a patent is sought. This declaration is directed to the international application of which it forms a part (if filing declaration with application). This declaration is directed to international application No. PCT/ . . . . . (if furnishing declaration pursuant to Rule 26ter). I hereby declare that my residence, mailing address, and citizenship are as stated next to my name. I hereby state that I have reviewed and understand the contents of the above-identified international application, including the claims of said application. I have identified in the request of said application, in compliance with PCT Rule 4.10, any claim to foreign priority, and I have identified below, under the heading "Prior Applications", by application number, country or Member of the World Trade Organization, day, month, and year of filing, any application for a patent or inventor's certificate filed in a country other than the United States of America, including any PCT international application designating at least one country other than the United States of America, having a filing date before that of the application on which foreign priority is claimed.
VIII-4-1-1	Prior applications:	

		I hereby acknowledge the duty to disclose information that is known by me to be material to patentability as defined by 37 C.F.R. § 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the PCT international filing date of the continuation-in-part application. 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 Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.
VIII-4-1-1-1	Name (LAST, First)	SELGERT, Franklin
VIII-4-1-1-2	Residence: (city and either US State, if applicable, or country)	Berkel en Rodenrijs, Netherlands
VIII-4-1-1-3	Mailing address:	Penningslaan 30 2651 BL Berkel en Rodenrijs Netherlands
VIII-4-1-1-4	Citizenship:	NL
VIII-4-1-1-5	Inventor's Signature: (The signature must be that of the inventor, not that of the agent)	/Franklin Selgert/
VIII-4-1-1-6	Date:	15 December 2009 (15.12.2009)
VIII-4-1-2-1	Name (LAST, First)	MULLER, Frank
VIII-4-1-2-2	Residence: (city and either US State, if applicable, or country)	Delft, Netherlands
VIII-4-1-2-3	Mailing address:	Hopstraat 39 2611 TB Delft Netherlands
VIII-4-1-2-4	Citizenship:	NL
VIII-4-1-2-5	Inventor's Signature: (The signature must be that of the inventor, not that of the agent)	/Frank Muller/
VIII-4-1-2-6	Date	15 December 2009 (15.12.2009)

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
13/139,433	08/15/2011	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ 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		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	06/13/2011									
	Total (37 CFR 1.16(i))	* 18	Minus	** 20	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 5	Minus	***5	= 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:
/DIANIECE JACOBS/

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.