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.
14/424,691	09/06/2016	9438572	4965.1017-000	1653

21005 7590 08/17/2016

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

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 0 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):

Antonius Norp, The Hague, NETHERLANDS;
Koninklijke KPN N.V., The Hague, NETHERLANDS;
Frank Fransen, Zuidhorn, NETHERLANDS;
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO, Den Haag, NETHERLANDS;
Sander De Kievit, Leiden, 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

14424691 - GAU: 2438

Receipt date: 03/16/2016 Sheet 1 of 2

Substitute for form 1449B/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** March 16, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

U.S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Number-Kind Code (if known)	ISSUE DATE / PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
/J.L./	1.	2015/0288724	~~10-25-2013~~ 10/2015	Fransen, et al.
/J.L./	2.	2011/0194460	08-11-2011	Witzel, et al.
/J.L./	3.	2013/0094638	04-18-2013	Anchan, Kirankumar
/J.L./	4.	2014/0067987	03-06-2014	Agrawal, et al.
/J.L./	5.	2006/0258383	11-16-2006	Jiang, et al.
	6.			
	7.			
	8.			
	9.			
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			

Change(s) applied to document, /C.S./ 5/26/2016

Copies of issued U.S. Patents and Published U.S. Applications are not required and are not being provided. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.

EXAMINER /Jason Lee/	DATE CONSIDERED 04/28/2016

2311520.v1

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)

21005 7590 05/11/2016
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

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.
14/424,691	02/27/2015	Antonius Norp	4965.1017-000	1653

TITLE OF INVENTION: Establishing A Device-To-Device Communication Session

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	08/11/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEE, JASON T	2438	726-004000

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 Hamilton, Brook, Smith & Reynolds, P.C.
(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)
Koninklijke KPN N.V.	The Hague, Netherlands
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO	Den Haag, 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 08-0380 (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 /Timothy J. Meagher, Reg. No. 39302/ Date 8/2/2016

Typed or printed name Timothy J. Meagher Registration No. 39,302

ERICSSON EXHIBIT 1002, Page 3

Electronic Patent Application Fee Transmittal

Application Number:	14424691
Filing Date:	27-Feb-2015
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Filer:	Timothy J. Meagher/Jennifer Torpey
Attorney Docket Number:	4965.1017-000

Filed as Large Entity

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	26519634
Application Number:	14424691
International Application Number:	
Confirmation Number:	1653
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Customer Number:	21005
Filer:	Timothy J. Meagher/Jennifer Torpey
Filer Authorized By:	Timothy J. Meagher
Attorney Docket Number:	4965.1017-000
Receipt Date:	02-AUG-2016
Filing Date:	27-FEB-2015
Time Stamp:	18:05:36
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	5084
Deposit Account	080380
Authorized User	Torpey, Jennifer

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 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	49651017000_IssueFeeTransmittal3.pdf	969426 93871549f27025fbe88871340b39124b80e95ee8	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30270 8ab124e0a8ca92cee1dc59095f3caa3c8a1c567c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	999696		

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 05/23/2016

14424691 - GAU: 2438

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** May 23, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

U.S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Number-Kind Code (if known)	ISSUE DATE / PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
/J.L./	1.	2011/0252144 A1	10-13-2011	Tung, et al.
	2.			
	3.			
	4.			
	5.			
	6.			
	7.			
	8.			
	9.			
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			

Copies of issued U.S. Patents and Published U.S. Applications are not required and are not being provided. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.

EXAMINER /Jason Lee/	DATE CONSIDERED 05/26/2016

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** May 23, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Country Code-Number-Kind Code (if known)	DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
/J.L./	1.	WO 2010/150813	12-29-2010	Panasonic Electronic Works Co., Ltd.
/J.L./	2.	JP 2002 290397	10-04-2002	Iryo Joho Syst Kaihatsu CT
/J.L./	3.	JP 2012 502587	01-26-2012	QUALCOMM INCORPORATED
/J.L./	4.	JP 2011 147148	07-28-2011	QUALCOMM INCORPORATED
/J.L./	5.	JP 2009 512296	03-19-2009	TELEFONAKTIEBOLAGET LM ERICSSON
/J.L./	6.	JP 2008 539643	11-13-2008	NOKIA CORPORATION
/J.L./	7.	JP 2006 253837	09-21-2006	Sony Corp.
/J.L./	8.	JP 2006 238273	08-30-2006	Hitachi, Ltd.
/J.L./	9.	JP 2005 244534	08-09-2005	Hitachi, Ltd.
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			

EXAMINER /Jason Lee/	DATE CONSIDERED 05/26/2016

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.
14/424,691	02/27/2015	Antonius Norp	4965.1017-000	1653

21005 7590 06/01/2016

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER
LEE, JASON T

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
06/01/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing.department@hbsr.com
helpdesk@hbsr.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
14/424,691	27 February, 2015	NORP ET AL.	4965.1017-000

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER	
JASON LEE	
ART UNIT	PAPER
2438	20160526

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The IDS filed 05/23/2016 has been considered.

/JASON LEE/
Primary Examiner, Art Unit 2438

PTO-90C (Rev.04-03)

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.
14/424,691	02/27/2015	Antonius Norp	4965.1017-000	1653

21005 7590 05/25/2016

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
05/25/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing.department@hbsr.com
helpdesk@hbsr.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
14/424,691	27 February, 2015	NORP ET AL.	4965.1017-000

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER	
JASON LEE	
ART UNIT	PAPER
2438	20160519

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The IDS filed 05/06/2016 has been considered.

/JASON LEE/
Primary Examiner, Art Unit 2438

PTO-90C (Rev.04-03)

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** May 6, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

Examiner's Initials	Cite No.	**OTHER DOCUMENTS** *(Including Author, Title, Date, Pertinent Pages, Etc.)*
/J.L./	1.	"Proximity aware service consideration on lawful interception," *Institute For Information Industry (III),* TSG-SA WG1 Meeting #57, Kyoto, Japan (February 2012).
/J.L./	2.	"Anonymously multi-party communication interception," *Institute For Information Industry (III),* TSG-SA WG1 Meeting #57, Kyoto, Japan (February 2012).
/J.L./	3.	"Lawful Interception For 3G and 4G Networks," January 31, 2012, Retrieved from the Internet: URL:http://www.aqsacom.com/resources/pdf/Li-3G-4G-White.pdf
/J.L./	4.	3rd Generation Partnership Project: Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 11), 3GPP TS 36.300, V11.3.0 (September 2012).
/J.L./	5.	3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G security; Lawful interception architecture and functions (Release 11), 3GPP TS 33.107 V11.3.0 (September 2012).
/J.L./	6.	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for the Evolved Packet Systems (EPS) (Release 11), 3GPP TS 22.278 V11.6.0 (September 2012).
	7.	
	8.	
	9.	
	10.	
	11.	
	12.	
	13.	
	14.	
	15.	

***Copies of any U.S. Office Communications or non-published U.S. Patent Applications are not being provided because the examiner has access to such documents through PAIR. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.**

EXAMINER /Jason Lee/	DATE CONSIDERED 05/19/2016

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** May 23, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

U.S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Number-Kind Code (if known)	ISSUE DATE / PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
	1.	2011/0252144 A1	10-13-2011	Tung, et al.
	2.			
	3.			
	4.			
	5.			
	6.			
	7.			
	8.			
	9.			
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			

Copies of issued U.S. Patents and Published U.S. Applications are not required and are not being provided. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.

EXAMINER	DATE CONSIDERED

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** May 23, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Country Code-Number-Kind Code (if known)	DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
	1.	WO 2010/150813	12-29-2010	Panasonic Electronic Works Co., Ltd.
	2.	JP 2002 290397	10-04-2002	Iryo Joho Syst Kaihatsu CT
	3.	JP 2012 502587	01-26-2012	QUALCOMM INCORPORATED
	4.	JP 2011 147148	07-28-2011	QUALCOMM INCORPORATED
	5.	JP 2009 512296	03-19-2009	TELEFONAKTIEBOLAGET LM ERICSSON
	6.	JP 2008 539643	11-13-2008	NOKIA CORPORATION
	7.	JP 2006 253837	09-21-2006	Sony Corp.
	8.	JP 2006 238273	08-30-2006	Hitachi, Ltd.
	9.	JP 2005 244534	08-09-2005	Hitachi, Ltd.
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			

EXAMINER	DATE CONSIDERED

Electronic Patent Application Fee Transmittal

Application Number:	14424691
Filing Date:	27-Feb-2015
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Filer:	Timothy J. Meagher/Jennifer Torpey
Attorney Docket Number:	4965.1017-000

Filed as Large Entity

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

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:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	25852180
Application Number:	14424691
International Application Number:	
Confirmation Number:	1653
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Customer Number:	21005
Filer:	Timothy J. Meagher/Jennifer Torpey
Filer Authorized By:	Timothy J. Meagher
Attorney Docket Number:	4965.1017-000
Receipt Date:	23-MAY-2016
Filing Date:	27-FEB-2015
Time Stamp:	16:20:40
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	$180
RAM confirmation Number	2948
Deposit Account	080380
Authorized User	HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

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 CFR 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 Letter	49651017000_IDS_Transmittal.pdf	90878 7262e7175cf63395be0bc06f4e564e513c441df0	no	3
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	49651017000_1449.pdf	91706 933b0702d4c20770d8e54b88581ea9d6d4a3b1f0	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	JP_2005_244534_Abstract.pdf	24261 8e595cb67bd2d2c9d3c2af3670fb71ed7be12d84	no	1
Warnings:					
Information:					
4	Foreign Reference	WO2010150813A1.pdf	2634864 aa48ed749899f6abff272e7fb9ee798210955a76	no	74
Warnings:					
Information:					
5	Foreign Reference	JP_2002_290397A_Abstract.pdf	889793 29564c770892a574599c22aa811e3b82a1d9dac9	no	15
Warnings:					
Information:					
6	Foreign Reference	JP_2006_253837_final.pdf	7033377 587618eb53106f289f83266f64b83b57ecc5e8a9	no	9
Warnings:					
Information:					
7	Foreign Reference	JP_2012_502587A_Abstract.pdf	1958575 f1dc5627ba3bfdac6d42fc27115859696837 4522	no	45
Warnings:					
Information:					

8	Foreign Reference	JP_2011_147148A.pdf	1383784 317a09a0f7c0d7573be0ae384f4749560fa51c26	no	33
Warnings:					
Information:					
9	Foreign Reference	JP_2009_512296A.pdf	511801 47c976639fe890baebeb996848ffd5000d3bdd47	no	2
Warnings:					
Information:					
10	Foreign Reference	JP_2008_539643A.pdf	1484618 f4f7fbb485506dde2ea20e7a5901ea8a8b9d7fa6	no	34
Warnings:					
Information:					
11	Foreign Reference	JP_2006_238273A.pdf	1438578 3b7d12588ee60cd4288699e3d8151f3c5a167138	no	31
Warnings:					
Information:					
12	Fee Worksheet (SB06)	fee-info.pdf	30242 3cc7d324b4a0b7752e0ca31570074a3ae57e7f5e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	17572477		

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

Inventors:	Antonius Norp, Frank Fransen and Sander De Kievit		
Application No.:	14/424,691	Group:	2438
Filed:	August 29, 2013	Examiner:	Lee, Jason T.
Confirmation No.:	1653		
For:	Establishing A Device-To-Device Communication Session		

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or is being facsimile transmitted to the United States Patent and Trademark Office on:

Date _____ Signature _____

Typed or printed name of person signing certificate

TRANSMITTAL LETTER FOR INFORMATION DISCLOSURE STATEMENT

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

Commissioner:

This Information Disclosure Statement is submitted:

☐ under 37 CFR 1.97(b), or
(Within any one of the following time periods: three months of filing national application (other than a CPA) or date of entry of the national stage in an international application; or before the mailing date of a first office action on the merits; or before the mailing of a first office action after the filing of a Request for Continued Examination)

☐ under 37 CFR 1.97(c) together with either:
- ☐ a Statement under 37 CFR 1.97(e), as checked below, or
- ☐ a $[180/90/45] fee under 37 CFR 1.17(p), or
(After the 37 CFR 1.97(b) time period, but before any of a final action, notice of allowance, or an action that closes prosecution, whichever occurs first)

☒ under 37 CFR 1.97(d) together with:
- ☒ a Statement under 37 CFR 1.97(e), as checked below, and
- ☒ a $180 fee under 37 CFR 1.17(p), or
(Filed after final action, notice of allowance, or an action that otherwise closes prosecution, but on or before payment of the issue fee)

☐ under 37 CFR 1.97(i):
Applicant requests that the IDS and cited reference(s) be placed in the application file.
(Filed after payment of issue fee)

No aspect of this submission constitutes a disclaimer of claim scope.

Statement Under 37 CFR 1.97(e)

☒ Each item of information contained in this 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 this Information Disclosure Statement; or

☐ No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, 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 this Information Disclosure Statement.

Statement Under 37 CFR 1.704(d) (Patent Term Adjustment)
Applies to original applications (other than design) filed on or after May 29, 2000

☐ (1) A paper containing only an information disclosure statement in compliance with §§ 1.97 and 1.98 will not be considered a failure to engage in reasonable efforts to conclude prosecution (processing or examination) of the application under paragraphs (c)(6), (c)(8), (c)(9), or (c)(10) of this section if it is accompanied by a statement that each item of information contained in the information disclosure statement:

☐ (i) Was first cited in any communication from a patent office in a counterpart foreign or international application or from the Office, and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the information disclosure statement; or

☐ (ii) Is a communication that was issued by a patent office in a counterpart foreign or international application or by the Office, and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the information disclosure statement.

☒ Enclosed herewith is a Listing of References. Copies of the cited references are enclosed except as indicated below or in the attached Listing of References.

☐ Copies of the cited references submitted with an Information Disclosure Statement in prior application, U.S. Application No. [ ], to which priority under 35 U.S.C. 120 is claimed, are not required under 37 CFR 1.98(d)(1) and (2) and are thus not provided.

☐ The listed references were cited in the enclosed Search Report in counterpart foreign application [add application number], which is listed in the attached Listing of References.

☒ The "concise explanation" requirement (non-English references) for foreign reference(s) 1 through 9, under 37 CFR 1.98(a)(3) is satisfied by:

- ☐ the explanation provided on the attached sheet.
- ☐ the explanation provided in the Specification.
- ☐ submission of the enclosed International Search Report.
- ☐ submission of the enclosed English-language version of a foreign Search Report and/or foreign Office Action.
- ☒ the enclosed English language abstract.

Method of payment:

☐ Authorization is NOT granted to charge any fees which may be due in this matter to our Deposit Account.

☒ Please charge Deposit Account 08-0380 in the amount of $180.

☐ A check for the fee noted above is enclosed, or the fee has been included in the check with the accompanying Reply.

☒ Please charge any deficiency in fees and credit any overpayment to Deposit Account 08-0380.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By /Timothy J. Meagher, Reg. No. 39,302/

Timothy J. Meagher
Registration No. 39,302
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: May 23, 2016

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

21005 7590 05/11/2016
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER
LEE, JASON T

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 05/11/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/424,691	02/27/2015	Antonius Norp	4965.1017-000	1653

TITLE OF INVENTION: Establishing A Device-To-Device Communication Session

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	08/11/2016

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)

21005 7590 05/11/2016
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

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.
14/424,691	02/27/2015	Antonius Norp	4965.1017-000	1653

TITLE OF INVENTION: Establishing A Device-To-Device Communication Session

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	08/11/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEE, JASON T	2438	726-004000

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. _____

ERICSSON EXHIBIT 1002, Page 26

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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.
14/424,691	02/27/2015	Antonius Norp	4965.1017-000	1653

21005 7590 05/11/2016

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 05/11/2016

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. 14/424,691	Applicant(s) NORP ET AL.	
	Examiner JASON LEE	Art Unit 2438	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 *3/16/16*.
   ☐ 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 *18-34*. 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 3/16/16
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *4/26/16* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JASON LEE/
Primary Examiner, Art Unit 2438

DETAILED ACTION

1. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.

2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

3. Applicant filed the response on March 16, 2016 for the office action dated December 10, 2015. The applicant amended claims 18 and 32-34. No claim is added. Claims 1-17 are canceled previously. As the result of Examiner's amendment in the instant office action, Claims 18, 30 and 32-34 are amended. Claims 18-34 are renumbered as 1-17 are pending.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 3/16/2016 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. Authorization for this examiner's amendment

was given in a telephone interview with Mr. Timothy J. Meagher (Reg. # 39,302) on 04/26/2016.

1. - 17. (Cancelled)

18. (Currently Amended) Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:

preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and on each of the mobile devices:

verifying a validity of the initiation key based on a current time;

requesting a further initiation key via the mobile network if no initiation key is deemed valid;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices; and

establishing the D2D communication session over the D2D communication channel based on the session key.

30. (Currently Amended) Method according to claim 18, further comprising requesting a further initiation key via the mobile network if ~~i) no initiation key is~~

~~deemed valid, or ii)~~ the key agreement procedure fails in providing the session key.

32. (Currently Amended) A non-transitory computer-readable medium configured to store instructions for, upon execution of the instructions on a mobile device, causing the mobile device to establish a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, by:

storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period;

verifying a validity of the initiation key based on a current time;

requesting a further initiation key via the mobile network if no initiation key is deemed valid;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and

establishing the D2D communication session over the D2D communication channel based on the session key.

33. (Currently Amended) Mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:

a storage area for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and

a computing subsystem for:

verifying a validity of the initiation key based on a current time;

requesting a further initiation key via the mobile network if no initiation key is deemed valid;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and

a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

34. (Currently Amended) Mobile network arranged for preloading an initiation key on a mobile device when the mobile device is connected to the mobile network, the initiation key being associated with a validity period, the mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to the mobile network, the mobile device comprising:

a computing subsystem for:

verifying a validity of the initiation key based on a current time;

requesting a further initiation key via the mobile network if no initiation key is deemed valid;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and

a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

Response to Arguments

6. Applicant's amendments are sufficient to overcome the claim rejections of the 35 USC 101 for claim 32 set forth in the previous office action. Applicant amended claim 32 with "non-transitory computer-readable medium" to tie the claim with statutory subject matter. Therefore, the claim rejections of the 35 USC 101 for claim 32 is withdrawn.

7. Applicant's amendments are sufficient to overcome the claim rejections of the 35 USC 112, 4th paragraph for claims 32 and 34 set forth in the previous office action. Applicant amended claims 32 and 34 with independent fashion. Therefore, the claim rejections of the 35 USC 112, 4th paragraph for claims 32 and 34 are withdrawn.

8. Applicant's amendments are sufficient to overcome the claim rejections of the 35 USC 112, 2nd paragraph for claims 18 and 33 set forth in the previous office action. Applicant amended claims 18 and 33 with clear language for the claimed limitations. Therefore, the claim rejections of the 35 USC 112, 2nd paragraph for claims 18 and 33 are withdrawn.

9. Applicant's arguments filed 03/16/2016 and telephone interview on 04/26/2016 have been fully considered and they are persuasive.

Allowable Subject Matter

10. Newly amended independent claims 18, 32, 33, and 34 is allowed over prior arts of record. Dependent claims 19-31 depend on the above-mentioned independent claim 18 are allowed by virtue of its dependency.

Examiner's statement of reasons for allowance

11. The following is an examiner's statement of reasons for allowance:

Newly amended independent claim 18 is allowed in view of the (examiner's) amendment and for reasons argued by applicant in pages 8-10 of the Remarks, filed 03/16/2016. Prior art of record, Hakola et al (U.S. Patent Publication US 2013/0013926 A1); in view of Vanderveen et al (U.S. Patent Publication US 2013/0227655 A1) fails to teach alone, at the time of the invention, the claimed features and limitations. The prior art of record does not teach or made obvious the feature of "in establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network" to "preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and on each of the mobile devices"; "verifying a validity of the initiation key based on a current time"; "requesting a further initiation key via the mobile network if no initiation key is deemed valid"; and "if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices"; and "establishing the D2D communication session over the D2D communication channel based on the session key" as recited in claim 18.

The prior art of record, 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. Therefore, claim 18 is considered to be allowable. Independent claims

32, 33, and 34 recite similar to claim 18, therefore, Independent claims 32, 33, and 34 are considered to be allowable.

Examiner performed updated search and additional search does not yield other specific references that reasonably, either singularly or in combination with cited references, would result a proper rejection that would have anticipated or made obvious all the steps disclosed in the independent claims 18, 32, 33, and 34 with proper motivation at or before the time it was effectively filed.

Dependent claims 19-31 depend upon the above-mentioned allowed claim 18 are therefore allowed by virtue of its dependency.

None of the prior art of record, 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 payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance."

Conclusion

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

a. "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol"; M Zhang et al; Wireless Communications, IEEE Transactions on 2005; 9 pages; discloses "a communication will be protected via established keys and

consequently initiates a resynchronization and key agreement procedures based on unused authentication vectors to protect security and enhancement of 3GPP communication."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. 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.

/JASON LEE/

Primary Examiner, Art Unit 2438

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	14/424,691	NORP ET AL.	
	Examiner	Art Unit	
	JASON LEE	2438	

All participants (applicant, applicant's representative, PTO personnel):

(1) *JASON LEE*. (3)_____.

(2) *Mr. Timothy J. Meagher (Reg. # 39,302)* . (4)_____.

Date of Interview: *26 April 2016*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *n/a*.

Identification of prior art discussed: *n/a*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

The examiner confirmed authorization from Attorney of record Mr. Timothy J. Meagher (Reg. # 39,302) to implement Examiner's Amendment based on Applicant's proposed examiner's amendment submitted by email on 04/26/2016..

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/JASON LEE/ Primary Examiner, Art Unit 2438	

Notice of References Cited	Application/Control No. 14/424,691	Applicant(s)/Patent Under Reexamination NORP ET AL.	
	Examiner JASON LEE	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
	A	US-				
	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	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	"Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol"; M Zhang et al; - Wireless Communications, IEEE Transactions on, 2005; 9 pages
	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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

14424691 - GAU: 2438

Receipt date: 03/16/2016 Sheet 1 of 2

Substitute for form 1449B/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** March 16, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

U.S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Number-Kind Code (if known)	ISSUE DATE / PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
/J.L./	1.	2015/0288724	10-25-2013	Fransen, et al.
/J.L./	2.	2011/0194460	08-11-2011	Witzel, et al.
/J.L./	3.	2013/0094638	04-18-2013	Anchan, Kirankumar
/J.L./	4.	2014/0067987	03-06-2014	Agrawal, et al.
/J.L./	5.	2006/0258383	11-16-2006	Jiang, et al.
	6.			
	7.			
	8.			
	9.			
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			

Copies of issued U.S. Patents and Published U.S. Applications are not required and are not being provided. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.

EXAMINER /Jason Lee/	DATE CONSIDERED 04/28/2016

Substitute for form 1449B/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** March 16, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

Examiner's Initials	Cite No.	**OTHER DOCUMENTS** *(Including Author, Title, Date, Pertinent Pages, Etc.)*
/J.L./	1.	Non-Final Office Action for U.S. Application No: 14/438,786, mailed on October 2, 2015. (Attorney Docket No: 3795.1018-000).
/J.L./	2.	3GPP TSG-SA WG1 Meeting #57, "Proximity Aware Service Consideration on Lawful Interception", Kyoto Japan, February 17, 2012.
	3.	
	4.	
	5.	
	6.	
	7.	
	8.	
	9.	
	10.	
	11.	
	12.	
	13.	
	14.	
	15.	
	16.	
	17.	
	18.	

***Copies of any U.S. Office Communications or non-published U.S. Patent Applications are not being provided because the examiner has access to such documents through PAIR. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.**

EXAMINER	/Jason Lee/	DATE CONSIDERED	04/28/2016

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14424691	NORP ET AL.
	Examiner	**Art Unit**
	JASON LEE	2438

CPC								
Symbol							**Type**	**Version**
H04L		63	/	062			F	2013-01-01
H04W		12	/	04			I	2013-01-01
H04W		76	/	023			I	2013-01-01
H04W		92	/	18			A	2013-01-01
H04L		63	/	061			I	2013-01-01
H04L		67	/	141			I	2013-01-01
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					

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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	17	
/JASON LEE/ Primary Examiner.Art Unit 2438	04/28/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14424691	NORP ET AL.
	Examiner	**Art Unit**
	JASON LEE	2438

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

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
713	168	171			

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	17	
/JASON LEE/ Primary Examiner.Art Unit 2438	04/28/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14424691	NORP ET AL.
	Examiner	**Art Unit**
	JASON LEE	2438

☐ 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		17	16	33										
	2	1	18	17	34										
	3	2	19												
	4	3	20												
	5	4	21												
	6	5	22												
	7	6	23												
	8	7	24												
	9	8	25												
	10	9	26												
	11	10	27												
	12	11	28												
	13	12	29												
	14	13	30												
	15	14	31												
	16	15	32												

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 17	
/JASON LEE/ Primary Examiner.Art Unit 2438 (Primary Examiner)	04/28/2016 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14424691	NORP ET AL.
	Examiner	Art Unit
	JASON LEE	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/01/2015	04/28/2016							
	1	-	-							
	2	-	-							
	3	-	-							
	4	-	-							
	5	-	-							
	6	-	-							
	7	-	-							
	8	-	-							
	9	-	-							
	10	-	-							
	11	-	-							
	12	-	-							
	13	-	-							
	14	-	-							
	15	-	-							
	16	-	-							
	17	-	-							
1	18	✓	=							
2	19	✓	=							
3	20	✓	=							
4	21	✓	=							
5	22	✓	=							
6	23	✓	=							
7	24	✓	=							
8	25	✓	=							
9	26	✓	=							
10	27	✓	=							
11	28	✓	=							
12	29	✓	=							
13	30	✓	=							
14	31	✓	=							
15	32	✓	=							
16	33	✓	=							
17	34	✓	=							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	"20150222612".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 15:46
S2	2	"20070253376".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:02
S3	3	"20130013926".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:14
S4	0	"200800209440".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:19
S5	2	"20080209440".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:20
S6	2	"20130227655".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:24
S7	0	"2009320102".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:30
S8	2	"20090320102".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:30
S9	3	"20080095361".pn.	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/11/28 16:31

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S10	2	("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (mobile) and (device-to-device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:00
S11	2	("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (mobile) and (device-to-device) and key	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:14
S12	2	"20130013926".pn. and (key with value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:18
S13	1	("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (key same (validity with (time or period)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:23
S14	0	"20130013926".pn. and ((key with session) same generat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:35
S15	0	"20130013926".pn. and ((key with session) same2 generat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:35
S16	0	"20130013926".pn. and ((key with session) and generat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:35
S17	1	"20130013926".pn. and ((session) and generat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:36
S18	4	"20130013926".pn. or "20130227655".pn. and (disabl$3 or delet$3 or eras$3 or remov$3 or cancel$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:46
S19	4	"20130013926".pn. or "20130227655".pn. and (different or	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/12/01 12:49

		overlap$4)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S20	2	("20130013926".pn. or "20130227655".pn.) and (different or overlap$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:49
S21	0	("20130013926".pn. or "20130227655".pn.) and (virtual)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:53
S22	1	("20130013926".pn. or "20130227655".pn.) and (virtual or identity)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:54
S23	0	("20130013926".pn. or "20130227655".pn.) and (count)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:58
S24	5	("20130013926".pn. or "20130227655".pn.) and (count or us$3 or limit$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:58
S25	1	("20130013926".pn. or "20130227655".pn.) and ((shared secret) or Diffie)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:11
S26	1	("20130013926".pn. or "20130227655".pn.) and ((shared secret) or Diffie or pass)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:13
S27	2	("20130013926".pn. or "20130227655".pn.) and ((request)same key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:15
S28	0	"20070253376".pn. and usage	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:22
S29	0	"20070253376".pn. and (usage or count)	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/12/01 13:23

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S30	1	"20090320102".pn. and (usage or count)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:24
S31	0	"20080095361".pn. and (usage or count)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:25
S32	0	h04l63/61.cpci.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:11
S33	6136	h04l63/061.cpci.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:11
S34	6838	h04l63/062.cpci.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:11
S35	354	S33 and S34	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:12
S36	301	S35 and @ad < "20120906"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:12
S37	0	S36 and ((mobile) and (device-to-device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:13
S38	103	S36 and ((mobile) or (device-to-device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:13
S39	7350	h04w76/023.cpci.	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/12/01 14:14

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S40	0	S38 and S39	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:14
S41	0	S36 and S39	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:15
S42	3271	S39 and @ad < "20120906"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:15
S43	436	S42 and (device-to-device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:16
S44	0	S43 and (key with usage)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:16
S45	0	S43 and (key same usage)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:17
S46	10	S36 and (key same usage)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:17
S47	0	S36 and (key same2 (usage with count))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:20
S48	0	S36 and (usage with count)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:20
S49	613	(key same (usage with count))	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/12/01 14:21

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S50	470	S49 and @ad < "20120906"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:22
S51	8	S50 and (S33 or S34)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:23

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	(((mobile) or (device-to-device)) with valid$3) and ((initiation key) with valid$3) with (key agreement).clm.	US-PGPUB; USPAT	ADJ	ON	2016/04/28 10:10

4/28/2016 10:24:00 AM
C:\Users\jlee16\Documents\EAST\Workspaces\14424691-112815.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14424691	NORP ET AL.
	Examiner	Art Unit
	JASON LEE	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
h04l63/061.cpci.;h04l63/062.cpci.	11/30/15	JL

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	4	11/28/15	JL
713	171	11/28/15	JL

SEARCH NOTES		
Search Notes	Date	Examiner
EAST searched, google patent searched	11/28/15	JL
inventer name and assignee searched	11/28/16	JL
"20090320102".pn. and (usage or count);("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (key same (validity with (time or period)));"20130013926".pn. and ((session) and generat$3);("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (mobile) and (device-to-device);h04l63/061.cpci.;h04l63/062.cpci.;(key same (usage with count));	11/28/15	JL
google searched with authentication with key agreement protocol	4/28/16	JL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
726	4	4/28/16	JL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
	(((mobile) or (device-to-device)) with valid$3) and ((initiation key) with valid$3) with (key agreement).clm.	4/28/16	JL

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** May 6, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

Examiner's Initials	Cite No.	**OTHER DOCUMENTS** *(Including Author, Title, Date, Pertinent Pages, Etc.)*
	1.	"Proximity aware service consideration on lawful interception," *Institute For Information Industry (III),* TSG-SA WG1 Meeting #57, Kyoto, Japan (February 2012).
	2.	"Anonymously multi-party communication interception," *Institute For Information Industry (III),* TSG-SA WG1 Meeting #57, Kyoto, Japan (February 2012).
	3.	"Lawful Interception For 3G and 4G Networks," January 31, 2012, Retrieved from the Internet: URL:http://www.agsacom.com/resources/pdf/Li-3G-4G-White.pdf
	4.	3rd Generation Partnership Project: Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 11), 3GPP TS 36.300, V11.3.0 (September 2012).
	5.	3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G security; Lawful interception architecture and functions (Release 11), 3GPP TS 33.107 V11.3.0 (September 2012).
	6.	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for the Evolved Packet Systems (EPS) (Release 11), 3GPP TS 22.278 V11.6.0 (September 2012).
	7.	
	8.	
	9.	
	10.	
	11.	
	12.	
	13.	
	14.	
	15.	

***Copies of any U.S. Office Communications or non-published U.S. Patent Applications are not being provided because the examiner has access to such documents through PAIR. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.**

EXAMINER	DATE CONSIDERED

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors:	Antonius Norp, Frank Fransen and Sander De Kievit		
Application No.:	14/424,691	Group:	2438
Filed:	August 29, 2013	Examiner:	Lee, Jason T.
Confirmation No.:	1653		
For:	Establishing A Device-To-Device Communication Session		

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or is being facsimile transmitted to the United States Patent and Trademark Office on:

Date _____ Signature _____

Typed or printed name of person signing certificate

TRANSMITTAL LETTER FOR SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

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

Commissioner:

This Information Disclosure Statement is submitted:

☐ under 37 CFR 1.97(b), or
(Within any one of the following time periods: three months of filing national application (other than a CPA) or date of entry of the national stage in an international application; or before the mailing date of a first office action on the merits; or before the mailing of a first office action after the filing of a Request for Continued Examination)

☒ under 37 CFR 1.97(c) together with either:
- ☐ a Statement under 37 CFR 1.97(e), as checked below, or
- ☒ a $180 fee under 37 CFR 1.17(p), or
(After the 37 CFR 1.97(b) time period, but before any of a final action, notice of allowance, or an action that closes prosecution, whichever occurs first)

☐ under 37 CFR 1.97(d) together with:
- ☐ a Statement under 37 CFR 1.97(e), as checked below, and
- ☐ a $[180/90/45] fee under 37 CFR 1.17(p), or
(Filed after final action, notice of allowance, or an action that otherwise closes prosecution, but on or before payment of the issue fee)

☐ under 37 CFR 1.97(i):
Applicant requests that the IDS and cited reference(s) be placed in the application file.
(Filed after payment of issue fee)

No aspect of this submission constitutes a disclaimer of claim scope.

Statement Under 37 CFR 1.97(e)

☐ Each item of information contained in this 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 this Information Disclosure Statement; or

☐ No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, 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 this Information Disclosure Statement.

Statement Under 37 CFR 1.704(d) (Patent Term Adjustment)
Applies to original applications (other than design) filed on or after May 29, 2000

☐ (1) A paper containing only an information disclosure statement in compliance with §§ 1.97 and 1.98 will not be considered a failure to engage in reasonable efforts to conclude prosecution (processing or examination) of the application under paragraphs (c)(6), (c)(8), (c)(9), or (c)(10) of this section if it is accompanied by a statement that each item of information contained in the information disclosure statement:

☐ (i) Was first cited in any communication from a patent office in a counterpart foreign or international application or from the Office, and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the information disclosure statement; or

☐ (ii) Is a communication that was issued by a patent office in a counterpart foreign or international application or by the Office, and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the information disclosure statement.

☒ Enclosed herewith is a Listing of References. Copies of the cited references are enclosed except as indicated below or in the attached Listing of References.

☐ Copies of the cited references submitted with an Information Disclosure Statement in prior application, U.S. Application No. [ ], to which priority under 35 U.S.C. 120 is claimed, are not required under 37 CFR 1.98(d)(1) and (2) and are thus not provided.

☐ The listed references were cited in the enclosed Search Report in counterpart foreign application [add application number], which is listed in the attached Listing of References.

☐ The "concise explanation" requirement (non-English references) for reference(s) [ ] under 37 CFR 1.98(a)(3) is satisfied by:

- ☐ the explanation provided on the attached sheet.
- ☐ the explanation provided in the Specification.
- ☐ submission of the enclosed International Search Report.
- ☐ submission of the enclosed English-language version of a foreign Search Report and/or foreign Office Action.
- ☐ the enclosed English language abstract.

Method of payment:

☐ Authorization is NOT granted to charge any fees which may be due in this matter to our Deposit Account.

☒ Please charge Deposit Account 08-0380 in the amount of $180.

☐ A check for the fee noted above is enclosed, or the fee has been included in the check with the accompanying Reply.

☒ Please charge any deficiency in fees and credit any overpayment to Deposit Account 08-0380.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By /Timothy J. Meagher, Reg. No. 39,302/
Timothy J. Meagher
Registration No. 39,302
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: May 6, 2016

Electronic Patent Application Fee Transmittal

Application Number:	14424691
Filing Date:	27-Feb-2015
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Filer:	Timothy J. Meagher/Jennifer Torpey
Attorney Docket Number:	4965.1017-000

Filed as Large Entity

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

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:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	25708877
Application Number:	14424691
International Application Number:	
Confirmation Number:	1653
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Customer Number:	21005
Filer:	Timothy J. Meagher/Jennifer Torpey
Filer Authorized By:	Timothy J. Meagher
Attorney Docket Number:	4965.1017-000
Receipt Date:	06-MAY-2016
Filing Date:	27-FEB-2015
Time Stamp:	17:07:17
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	$180
RAM confirmation Number	13844
Deposit Account	080380
Authorized User	HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

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 CFR 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	Non Patent Literature	3rd_Generation_Partnership_Project_3GPP_TS_22_278.pdf	845311 1c64e2d5ca5b629b5a921fc46f559d0785a0a90e	no	28
Warnings:					
Information:					
2	Non Patent Literature	3rd_Generation_Partnership_Project_3GPP_TS_33_107.pdf	2325963 5c7855bf1af8c9e08087fa7ed6a66c2fbb38a326	no	135
Warnings:					
Information:					
3	Non Patent Literature	3rd_Generation_Partnership_Project_3GPP_TS_36_300.pdf	11312642 bdd7d2a27d5084c7f319b8ceeebed0c982e4d877	no	205
Warnings:					
Information:					
4	Non Patent Literature	Anonymously_Multi_Party_Communication.pdf	173701 b5637dc35e1d736056e348246f6a5dfea02d3590	no	3
Warnings:					
Information:					
5	Non Patent Literature	Lawful_Interception_For_3G.pdf	2711652 0c44485024b1c442afde17b60f2bb2112ae183e4	no	38
Warnings:					
Information:					
6	Non Patent Literature	Proximity_Aware_Service.pdf	132733 21b11de7b62ad250bb16d580bdc094a6c25b080c	no	3
Warnings:					
Information:					
7	Information Disclosure Statement (IDS) Form (SB08)	49651017000_1449.pdf	111024 c2bfaf3077899505160673 4642e27c2e01fb3625	no	1
Warnings:					
Information:					

This is not an USPTO supplied IDS fillable form

8	Transmittal Letter	49651017000_IDS_Transmittal 2.pdf	90866 bb46dd77e5868735029918a21834e2af54e5f3c6	no	3
Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	30250 06b7ef8f45cd652b0959abe2f7ab7c09a511d12e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	17734142	

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

Inventors:	Antonius Norp, Frank Fransen and Sander De Kievit		
Application No.:	14/424,691	Group:	2438
Filed:	August 29, 2013	Examiner:	Lee, Jason T.
Confirmation No:	1653		
For:	Establishing A Device-To-Device Communication Session		

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or is being facsimile transmitted to the United States Patent and Trademark Office on:

_____ _____
Date Signature

_____
Typed or printed name of person signing certificate

AMENDMENT

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

Commissioner:

This Amendment is being filed in response to the Office Action mailed from the U.S. Patent and Trademark Office on December 10, 2015 in the above-identified application. Reconsideration and further examination are requested.

An extension of time to respond to the Office Action is respectfully requested. A Petition for Extension of Time and the appropriate fee are being filed concurrently with this Amendment.

Please amend the application as follows:

Amendments to the Claims

Please amend claims 18, 32, 33 and 34.

The Claim Listing below will replace all prior versions of the claims in the application:

Claim Listing

1. - 17. (Cancelled)

18. (Currently Amended) Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:

preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and on each of the mobile devices:

verifying a validity of the initiation key based on a current time;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key based on a match of the respective initiation keys ~~if the initiation key~~ used by each of the mobile devices ~~matches~~; and

establishing the D2D communication session over the D2D communication channel based on the session key.

19. (Previously Presented) Method according to claim 18, wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network.

20. (Previously Presented) Method according to claim 18, wherein the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device.

21. (Previously Presented) Method according to claim 20, wherein the secure storage area is provided by a trusted computing subsystem of each respective mobile device.

22. (Previously Presented) Method according to claim 21, wherein at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem.

23. (Previously Presented) Method according to claim 18, further comprising:

preloading a set of initiation keys on each of the mobile devices, the set of initiation keys key being associated with a respective set of validity periods; and

performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.

24. (Previously Presented) Method according to claim 23, further comprising:

preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys; and

performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.

25. (Previously Presented) Method according to claim 23, further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session.

26. (Previously Presented) Method according to claim 23, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods.

27. (Previously Presented) Method according to claim 18, wherein the initiation key is associated with a virtual network identity, and wherein the verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel.

28. (Previously Presented) Method according to claim 18, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and wherein the verifying the validity of the initiation key is further based on the usage count.

29. (Previously Presented) Method according to claim 28, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session.

30. (Previously Presented) Method according to claim 18, further comprising requesting a further initiation key via the mobile network if i) no initiation key is deemed valid, or ii) the key agreement procedure fails in providing the session key.

31. (Previously Presented) Method according to claim 18, wherein the key agreement procedure comprises:

a three-pass authentication procedure; or

a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.

32. (Currently Amended) A non-transitory computer-readable medium configured to store ~~Control software comprising~~ instructions for, upon execution of the ~~control software~~ instructions on a mobile device, causing the mobile device to establish ~~the~~ a device-to-device (D2D) communication session ~~according to the method of claim 18~~ with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, by:

storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period;

verifying a validity of the initiation key based on a current time;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and

establishing the D2D communication session over the D2D communication channel based on the session key.

33. (Currently Amended) Mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:

a storage area for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and

a computing subsystem for:

verifying a validity of the initiation key based on a current time;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device ~~and~~ matches an initiation key used by the further mobile device ~~matches~~; and

a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

34. (Currently Amended) Mobile network arranged for preloading an initiation key on a mobile device ~~according to claim 33~~ when the mobile device is connected to the mobile network, the initiation key being associated with a validity period, the mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to the mobile network, the mobile device comprising:

a computing subsystem for:

verifying a validity of the initiation key based on a current time;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure

with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and

a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

REMARKS

Amendments to the Claims

Claims 18-34 are pending in the application. With entry of the amendment, claims 18 and 32-34 are being amended.

The amendments are made to expedite prosecution of this application. Applicant is not conceding that the claims prior to amendment are not patentable. No inference should be made that Applicant is disclaiming any subject matter of the present application, and Applicant reserves the right to pursue the unamended claims or any other broader or narrower claims supported by the disclosure at a later date, including in one or more continuing applications. Cancellation of any claim herein is without prejudice to reinstatement in this or a continuing application.

Claim Rejections – 35 USC 101

Claim 32 is rejected under 35 U.S.C. 101. In particular, the Office notes the recitation "software comprising…", and concludes the claim is directed to non-statutory subject matter.

Applicant is amending claim 32 to recite "a non-transitory computer-readable medium" which is statutory subject matter.

Reconsideration of the rejection under 35 U.S.C. 101 is respectfully requested.

Claim Rejections – 35 USC 112, 4th paragraph

Claims 32 and 34 are rejected under 35 U.S.C. 112, 4th paragraph.

Applicant is amending claims 32 and 34 to remove claim dependency from respective claims 18 and 33.

Reconsideration of the rejections under 35 U.S.C. 112, 4th paragraph, is respectfully requested.

Claim Rejections – 35 USC 112, 2nd paragraph

Claims 18 and 33 are rejected under 35 U.S.C. 112, 2nd paragraph.

The Office indicates the view that recitation of "the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches" in claim 18 is unclear.

Applicant is amending claim 18 to recite "the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices."

The Office indicates the view that recitation of "the key agreement procedure resulting in the session key if the initiation key used by the mobile device and the further mobile device matches" in claim 33 is unclear.

Applicant is amending claim 33 to recite "the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device."

Reconsideration of the rejections under 35 U.S.C. 112, 2nd paragraph, is respectfully requested.

Claim Rejections – 35 USC 103

Claims 18-27 and 30-34 are rejected under 35 U.S.C. 103 as being unpatentable over Hakola et al. (US2013/0013926; hereinafter "Hakola") in view of Vanderveen et al. (US2013/0227655; hereinafter "Vanderveen"). Applicant respectfully disagrees.

The Office notes on page 7 of the Office Action the view that the recited "initiation key" of claim 18 is the same as the "base value" disclosed in Hakola, referring to Hakola [0004]. Applicant respectfully disagrees. A base value would not be reasonably interpreted by the skilled person as a key. Hakola [0004] discloses "generating a local device security key based on a secret key and a base value." The skilled person would understand the base value to be an input parameter for generating the local device security key. The base value is further elaborated in Hakola [0042] "… the eNB 120 may be configured to generate base values (e.g., base value_a and base value_b), which may be random or pseudo-random numbers." So indeed the base value is an input number and cannot be regarded as an initiation key.

Claim 18 requires that the initiation key is loaded on each of the mobile devices. However, Hakola discloses different keys for each mobile device. For example, this is clear from Hakola [0042] "The eNB 120 may be configured to subsequently send base value_a to mobile terminal 150a and base value_b to mobile terminal 150b, at 305a and 305b respectively." Thus, in Hakola there are different base values for each mobile device and consequently different keys for each mobile device. Also Hakola at [0043-0044] continues to generate different secret

keys for each mobile terminal. The wording "same secret key" in [0043] is used for generating the same key in the MME as for the mobile terminals. Nowhere in Hakola is it disclosed that mobile terminals use the same base values or secret keys. Therefore, Hakola does not disclose the feature of claim 18 "preloading an initiation key on each of the mobile devices."

At the bottom of page 6 of the Office Action, the Office indicates the view that the feature of "verifying a validity of the initiation key based on a current time" is allegedly present in Hakola, but the Office does not provide any support. Perhaps the same support is intended as used for the feature "the initiation key being associated with a validity period." However, Applicant respectfully disagrees that Hakola discloses either of these features. The mentioning in Hakola that "retrieval, loading, and execution of the program code instructions may be performed sequentially such that one instruction is retrieved, loaded and executed at a time," as noted by the Office at page 7 of the Office Action, does not imply in any way that a key would be valid at one time and invalid at a later time.

As the mobile devices in Hakola do not have the same initiation key, as to be expected, Hakola does not teach the feature of "generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices" as required in claim 18 as amended. This is simply not part of the teaching of Hakola.

Therefore, while Hakola may disclose a method for device-to-device key management using security keys, the method is very different from the method of claim 18 as amended. Vanderveen discloses authorization tickets having a validity time, but Vanderveen cannot cure the deficiencies in the teaching of Hakola. Using Hakola, and in view of Vanderveen, the skilled person would not arrive at the present invention of claim 18. Thus, claim 18 is patentable over the cited combination of Hakola and Vanderveen. Claims 32-34 recite similar features and are patentable for at least the same reasons given for claim 18. Claims 19-27 and 30-31 depend from claim 18 and are patentable for at least the same reasons.

Claims 28 and 29 are rejected under 35 U.S.C. 103 as being unpatentable over Hakola and Vanderveen and further in view of Ou (US2009/0320102). Applicant respectfully disagrees.

Ou does cure the deficiencies of Hakola and Vanderveen as noted above with respect to claim 18. Therefore, claims 28 and 29, which depend from claim 18, are patentable over the cited combination for at least the reasons given for claim 18.

Reconsideration of the rejections under 35 U.S.C. 103 is respectfully requested.

Information Disclosure Statement

An Information Disclosure Statement (IDS) is being filed concurrently herewith. Entry of the IDS is respectfully requested.

Payment of Fees

Authorization is hereby granted to charge the fees due with this submission, including any extension of time fee, to Deposit Account No. 08-0380.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By /Timothy J. Meagher, Reg. No. 39,302/
Timothy J. Meagher
Registration No. 39,302
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Date: 3/16/2016

Electronic Patent Application Fee Transmittal

Application Number:	14424691
Filing Date:	27-Feb-2015
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Filer:	Mary Lou Wakimura/Jennifer Torpey
Attorney Docket Number:	4965.1017-000

Filed as Large Entity

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Independent claims in excess of 3	1614	1	420	420
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	200	200
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**800**

Electronic Acknowledgement Receipt

EFS ID:	25207776
Application Number:	14424691
International Application Number:	
Confirmation Number:	1653
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Customer Number:	21005
Filer:	Mary Lou Wakimura/Jennifer Torpey
Filer Authorized By:	Mary Lou Wakimura
Attorney Docket Number:	4965.1017-000
Receipt Date:	16-MAR-2016
Filing Date:	27-FEB-2015
Time Stamp:	13:17:49
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	$800
RAM confirmation Number	10213
Deposit Account	080380
Authorized User	HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

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 CFR 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 Letter	49651017000_Transmittal_IDS.pdf	90844 ad03a63f42f2d64b88ec05f18a3962f1a53ee3cf	no	3
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	49651017000_LOR.pdf	111194 01812f4e45a27b6d4128b93df3dd2a6062b425e9	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	49651017000_NPL_Reference.PDF	32530 45b2e929fc1732a2cf73c4032bc0c557530f9421	no	1
Warnings:					
Information:					
4	Miscellaneous Incoming Letter	49651017000_Amendment_Transmittal.pdf	100192 ca0052f0581a66ea956b8c1543d125511f05dc8c	no	3
Warnings:					
Information:					
5		49651017000_Amendment2.pdf	93026 4d8e28b3f594706b72d04da57295a82dec892e16	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	10

Warnings:

Information:

6	Fee Worksheet (SB06)	fee-info.pdf	33958 b6cad3b3d1bed94651a419d6011a4248b901b384	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	461744

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

Inventors:	Antonius Norp, Frank Fransen and Sander De Kievit		
Application No.:	14/424,691	Group:	2438
Filed:	August 29, 2013	Examiner:	Lee, Jason T.
Confirmation No.:	1653		
For:	Establishing A Device-To-Device Communication Session		

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or is being facsimile transmitted to the United States Patent and Trademark Office on:

Date _____ Signature _____

Typed or printed name of person signing certificate

TRANSMITTAL LETTER FOR SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

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

Commissioner:

This Information Disclosure Statement is submitted:

☐ under 37 CFR 1.97(b), or
(Within any one of the following time periods: three months of filing national application (other than a CPA) or date of entry of the national stage in an international application; or before the mailing date of a first office action on the merits; or before the mailing of a first office action after the filing of a Request for Continued Examination)

☒ under 37 CFR 1.97(c) together with either:
- ☐ a Statement under 37 CFR 1.97(e), as checked below, or
- ☒ a $180 fee under 37 CFR 1.17(p), or
(After the 37 CFR 1.97(b) time period, but before any of a final action, notice of allowance, or an action that closes prosecution, whichever occurs first)

☐ under 37 CFR 1.97(d) together with:
- ☐ a Statement under 37 CFR 1.97(e), as checked below, and
- ☐ a $[180/90/45] fee under 37 CFR 1.17(p), or
(Filed after final action, notice of allowance, or an action that otherwise closes prosecution, but on or before payment of the issue fee)

☐ under 37 CFR 1.97(i):
Applicant requests that the IDS and cited reference(s) be placed in the application file.
(Filed after payment of issue fee)

No aspect of this submission constitutes a disclaimer of claim scope.

Statement Under 37 CFR 1.97(e)

☐ Each item of information contained in this 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 this Information Disclosure Statement; or

☐ No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, 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 this Information Disclosure Statement.

Statement Under 37 CFR 1.704(d) (Patent Term Adjustment)
Applies to original applications (other than design) filed on or after May 29, 2000

☐ (1) A paper containing only an information disclosure statement in compliance with §§ 1.97 and 1.98 will not be considered a failure to engage in reasonable efforts to conclude prosecution (processing or examination) of the application under paragraphs (c)(6), (c)(8), (c)(9), or (c)(10) of this section if it is accompanied by a statement that each item of information contained in the information disclosure statement:

☐ (i) Was first cited in any communication from a patent office in a counterpart foreign or international application or from the Office, and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the information disclosure statement; or

☐ (ii) Is a communication that was issued by a patent office in a counterpart foreign or international application or by the Office, and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the information disclosure statement.

☒ Enclosed herewith is a Listing of References. Copies of the cited references are enclosed except as indicated below or in the attached Listing of References.

☐ Copies of the cited references submitted with an Information Disclosure Statement in prior application, U.S. Application No. [ ], to which priority under 35 U.S.C. 120 is claimed, are not required under 37 CFR 1.98(d)(1) and (2) and are thus not provided.

☐ The listed references were cited in the enclosed Search Report in counterpart foreign application [add application number], which is listed in the attached Listing of References.

☐ The "concise explanation" requirement (non-English references) for reference(s) [ ] under 37 CFR 1.98(a)(3) is satisfied by:

- ☐ the explanation provided on the attached sheet.
- ☐ the explanation provided in the Specification.
- ☐ submission of the enclosed International Search Report.
- ☐ submission of the enclosed English-language version of a foreign Search Report and/or foreign Office Action.
- ☐ the enclosed English language abstract.

Method of payment:

☐ Authorization is NOT granted to charge any fees which may be due in this matter to our Deposit Account.

☒ Please charge Deposit Account 08-0380 in the amount of $180.

☐ A check for the fee noted above is enclosed, or the fee has been included in the check with the accompanying Reply.

☒ Please charge any deficiency in fees and credit any overpayment to Deposit Account 08-0380.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By /Timothy J. Meagher, Reg. No. 39,302/
Timothy J. Meagher
Registration No. 39,302
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 3/16/2016

Substitute for form 1449B/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** March 16, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

U.S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Number-Kind Code (if known)	ISSUE DATE / PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
	1.	2015/0288724	10-25-2013	Fransen, et al.
	2.	2011/0194460	08-11-2011	Witzel, et al.
	3.	2013/0094638	04-18-2013	Anchan, Kirankumar
	4.	2014/0067987	03-06-2014	Agrawal, et al.
	5.	2006/0258383	11-16-2006	Jiang, et al.
	6.			
	7.			
	8.			
	9.			
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			

Copies of issued U.S. Patents and Published U.S. Applications are not required and are not being provided. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.

EXAMINER	DATE CONSIDERED

Substitute for form 1449B/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** March 16, 2016 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	APPLICATION NO. 14/424,691	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER Lee, Jason T.	CONFIRMATION NO. 1653	GROUP 2438

Examiner's Initials	Cite No.	**OTHER DOCUMENTS** *(Including Author, Title, Date, Pertinent Pages, Etc.)*
	1.	Non-Final Office Action for U.S. Application No: 14/438,786, mailed on October 2, 2015. (Attorney Docket No: 3795.1018-000).
	2.	3GPP TSG-SA WG1 Meeting #57, "Proximity Aware Service Consideration on Lawful Interception", Kyoto Japan, February 17, 2012.
	3.	
	4.	
	5.	
	6.	
	7.	
	8.	
	9.	
	10.	
	11.	
	12.	
	13.	
	14.	
	15.	
	16.	
	17.	
	18.	

***Copies of any U.S. Office Communications or non-published U.S. Patent Applications are not being provided because the examiner has access to such documents through PAIR. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.**

EXAMINER	DATE CONSIDERED

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors: Antonius Norp, Frank Fransen and Sander De Kievit

Application No.: 14/424,691 Group: 2438

Filed: August 29, 2013 Examiner: Lee, Jason T.

Confirmation No.: 1653

For: Establishing A Device-To-Device Communication Session

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or is being facsimile transmitted to the United States Patent and Trademark Office on:

_____ _____

Date Signature

_____

Typed or printed name of person signing certificate

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

Commissioner:

Transmitted herewith is an Amendment for filing in the above-identified application.

☐ Small entity status of this application under 37 CFR 1.9 and 1.27 has been established by a Small Entity Statement previously submitted.

☐ A Small Entity Statement to establish small entity status under 37 CFR 1.9 and 1.27 is enclosed.

☐ The Assignee hereby asserts small entity status of the above-identified application under 37 CFR 1.27. This statement is being executed on behalf of the Assignee pursuant to 1.27(c)(2).
(Use if large entity and changing to small entity.)

☐ Applicant qualifies for and certifies micro entity status. A Certification of Micro Entity Status **[Option** (Gross Income Basis)(Institution of Higher Education Basis)**]** is enclosed.

The claims fee has been calculated as shown below:

	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR	PRESENT EXTRA	LARGE ENTITY RATE	LARGE ENTITY ADDIT. FEE
TOTAL	17	MINUS	* 20		X $80	$
INDEP	4	MINUS	** 3	1	X $420	$ 420
☐ FIRST PRESENTATION OF MULTIPLE DEP. CLAIM					+ $780	$

* not fewer than 20
** not fewer than 3

TOTAL OF ABOVE = $ 0

☐ Applicant asserts small entity status. Fees above are reduced by 50%. MINUS $ 0

☐ Applicant certifies micro entity status. Fees above are reduced by 75%. MINUS $ 0

TOTAL CLAIMS FEE $ 420

Petition for Extension of Time

☒ Applicant hereby petitions to extend the time to respond to the Office Action dated December 10, 2015 for one month from March 10, 2016 to April 10, 2016. The appropriate fee is set forth below.

Please charge Deposit Account No. 08-0380 for the following fees:

☒	Petition for one month Extension of Time	$ 200
☒	Claims Fee	$ 420
☒	Other Fees:	
	Information Disclosure Statement (IDS)	$ 180
		$
	TOTAL:	$ 800

A check is enclosed in payment of the following fees:

☐	Petition for [ ] month Extension of Time	$
☐	Claims Fee	$
☐	Other Fees:	
		$
		$
	TOTAL:	$

☒ Please charge any deficiency or credit any overpayment in the fees that may be due in this matter to Deposit Account No. 08-0380.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By /Timothy J. Meagher, Reg. No. 39,302/
Timothy J. Meagher
Registration No.: 39,302
Telephone (978) 341-0036
Facsimile (978) 341-0136

Concord, Massachusetts 01742-9133
Dated: 3/16/2016

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.
14/424,691	02/27/2015	Antonius Norp	4965.1017-000	1653

21005 7590 12/10/2015

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER
LEE, JASON T

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
12/10/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing.department@hbsr.com
helpdesk@hbsr.com

Office Action Summary	Application No. 14/424,691	Applicant(s) NORP ET AL.	
	Examiner JASON LEE	Art Unit 2438	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 *2/27/2015*.

☐ 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) *18-34* 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) *18-34* 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 *2/27/15* 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 *2/27/15*.

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. The original application is filed on 02/27/2015 with claims 1-17. A preliminary amendment is filed on February 27, 2015. Claims 1-17 are cancelled. Claims 18-34 are new. Therefore, Claims 18-34 are presented for examination.

Drawings

2. The drawings replacement filed on 02/27/2015 are accepted.

Oath/Declaration

3. For the record, the Examiner acknowledges that the Oath/Declaration submitted on 04/17/2015 has been accepted.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 02/27/2015 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Priority

5. This application is related to and claimed the benefits of EPO App. No. 12183256.2 filed on 09/06/2012.

Specification

6. For the record, the Examiner acknowledges that the amended [0001] for incorporating the information for the related applications submitted on 02/27/2015 has been accepted.

Claim Rejections - 35 USC § 101

7. 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.

8. Claim 32 is rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention.

9. Dependent claim 32 recites the limitation "software comprising instructions for, upon execution of the control software on a mobile device". The claimed subject matter is "software". Therefore, claim 32 is rejected under 35 U.S.C. §101 as covering non-statutory subject matter.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the fourth paragraph of 35 U.S.C. 112:

Subject to the [fifth paragraph of 35 U.S.C. 112], a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

11. Claims 32 and 34 are rejected under 35 U.S.C. 112, 4th paragraph, as being of improper dependent form for failing to further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends. Dependent claim 32 is a software claim which is not the same as the independent claim 18, which is a METHOD claim. Therefore, it is improper dependent claim because it mixed the category of invention (i.e. method and software). Thus, it is improper dependent claim because it mixed the category. Applicant may cancel the

claim(s), amend the claim(s) to place the claim(s) in proper dependent form, rewrite the claim(s) in independent form, or present a sufficient showing that the dependent claim(s) complies with the statutory requirements.

Similarly, claim 34 is a "mobile network" claim which is not the same as the independent claim 33, which is a mobile device claim. Thus, it is improper dependent claim because it mixed the category. Applicant may cancel the claim(s), amend the claim(s) to place the claim(s) in proper dependent form, rewrite the claim(s) in independent form, or present a sufficient showing that the dependent claim(s) complies with the statutory requirements.

12. 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.

13. Claims 18 and 33 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

14. Independent claim 18 recites: "the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices **matches".** The claim limitation is unclear. It is unclear because there is no recitation of what entity is been

matched and how the matching is done. Similarly, claim 33 has same issue. Therefore, Claims 18 and 33 are rendered unclear.

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

16. Claims 18-27, and 30-34 are rejected under 35 U.S.C. 103 as being unpatentable over Hakola et al (U.S. Patent Publication US 2013/0013926 A1; hereafter "Hakola") in view of Vanderveen et al (U.S. Patent Publication US 2013/0227655 A1; hereafter "Vanderveen").

> Examiner Notes: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including non-preferred embodiments. *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), *cert. denied,* 493 U.S. 975 (1989). See MPEP 2123.

As for claims 18, 32, 33 and 34:

Hakola discloses "a mobile terminal configured for device-to-device key management" in a cellular communication network (See Hakola FIG 6 and [0028-0031]). The communication network are directed to the generation, sharing, and utilization of security keys in the context of device-to-device (D2D) communications using encrypted

or secured connections. (See Hakola [0030-0032]) The local device security key may be configured for use in device-to-device communications. The example method may also include receiving a security key combination value, and deconstructing the security key combination value using the local device security key to determine a peer device security key. The peer device security key may be configured for use in device-to-device communications. (See Hakola [abstract], [0004-0005], and [0007-0009]). Hakola discloses "generating a local device security key based on a secret key and a base value" (See Hakola [0004]). By using the "base value" for the key, Hakola discloses "[T]he base values may be sent with a communication mode change command to trigger the mobile terminals 150 to transition to a D2D communications session, and, for example begin to establish the D2D connection 175" for "a D2D security key for use with D2D communications originating from mobile terminal". (See Hakola FIG 3 and [0042-0044]) and "establishing the D2D communication session over the D2D communication channel based on the session key" (See Hakola [0035-0036] and [0048-0049]). Therefore, Hakola discloses the claimed limitations of "**Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising: preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and on each of the mobile devices: verifying a validity of the initiation key based on a current time; if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key**

agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and establishing the D2D communication session over the D2D communication channel based on the session key." (Examiner's note: the "base value" for the device key is the "initiation key" as claimed)

Hakola also discloses "the flow of the D2D operation with flowcharts which shows in FIGS. 2-4 and 7-9", the operation of the method implementing the functions specified in the flowcharts' operations which "retrieval, loading, and execution of the program code instructions may be performed sequentially such that one instruction is retrieved, loaded, and executed at a time". Thus, Hokola teaches the time associated with the key. Hakola does not explicitly disclose "**the initiation key being associated with a validity period"** as claimed. However, Vanderveen teaches this limitation (See Vanderveen "validity time" (Vanderveen [0157] "Validating the second authorization ticket includes verifying both the validity time and the cryptographic signature. In accordance with some aspects, validating the second authorization ticket includes validating an identity of the second device as identified in the second authorization ticket, verifying possession of a private key associated with an identity and a public key included in a digital certification, or verifying a shared key derived through a mutual authentication process")

Vanderveen, like Hokola, is in the same field of endeavor of establish a valid

communication session between the wireless communications devices (See Vanderveen [0096]) discloses "**the initiation key being associated with a validity period"** as claimed as above. Vanderveen further discloses "**verifying a validity of the initiation key based on a current time"** (See Vanderveen [0051], [0059], [0066-0069] [0074] and [0094])

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to implement the teaching of Vanderveen with the invention of Hokola for a D2D communication session with mobile devices with a mutual authentication process for establishing a validated communication with the device based in part on the authorization validity time for further enhance the security of the cellular communication network. (See Vanderveen [0021-0024])

Claim 33 recites similar limitations to claim 18, mutatis mutandis, the subject matter of claim 33 which is therefore also considered to be taught by the combination of Hokola and Vanderveen as recited above.

Claims 32 and 34 recite similar limitations to claims 18 and 33, mutatis mutandis, the subject matter of claims 32 and 34 which are therefore also considered to be taught by the combination of Hokola and Vanderveen as recited above.

As for claim 19:

The combination of Hokola and Vanderveen discloses the **method according to claim 18** as above, **wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network.** (See Hokola [0030])

As for claim 20:

The combination of Hokola and Vanderveen discloses the **method according to claim 18** as above, **wherein the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device.** (See Hokola [0015], [0053-0055])

As for claim 21:

The combination of Hokola and Vanderveen discloses the **method according to claim 20** as above, **wherein the secure storage area is provided by a trusted computing subsystem of each respective mobile device.** (See Vanderveen [0014], [0052])

Examiner supplies the same rational for the combination of the reference as in claim 18 above.

As for claim 22:

The combination of Hokola and Vanderveen discloses the **method according to claim 21** as above, **wherein at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem.** (See Vanderveen [0052-0053])

Examiner supplies the same rational for the combination of the reference as in claim 18 above.

As for claim 23:

The combination of Hokola and Vanderveen discloses the **method according to claim 18** as above, **further comprising: preloading a set of initiation keys on each of the**

mobile devices, the set of initiation keys key being associated with a respective set of validity periods; and performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key. (See Vanderveen [0007])

Examiner supplies the same rational for the combination of the reference as in claim 18 above.

As for claim 24:

The combination of Hokola and Vanderveen discloses the **method according to claim 23** as above, **further comprising: preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys;** (See Hokola [0030]) **and performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.** (See Vanderveen [0007])

Examiner supplies the same rational for the combination of the reference as in claim 18 above.

As for claim 25:

The combination of Hokola and Vanderveen discloses the **method according to claim 23** as above, **further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session.** (See Vanderveen [0006])

Examiner supplies the same rational for the combination of the reference as in claim 18 above.

As for claim 26:

The combination of Hokola and Vanderveen discloses the **method according to claim 23** as above, **wherein the set of validity periods is constituted at least in part by different but overlapping validity periods.** (See Vanderveen [0057], [0059])

Examiner supplies the same rational for the combination of the reference as in claim 18 above.

As for claim 27:

The combination of Hokola and Vanderveen discloses the **method according to claim 18** as above, **wherein the initiation key is associated with a virtual network identity, and wherein the verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel.** (See Vanderveen [0063]-[0065])

Examiner supplies the same rational for the combination of the reference as in claim 18 above.

As for claim 30:

The combination of Hokola and Vanderveen discloses the **method according to claim 18** as above, **further comprising requesting a further initiation key via the mobile network if i) no initiation key is deemed valid, or ii) the key agreement procedure fails in providing the session key.** (See Hokola [0048] FIG 4, and [0061-0062])

As for claim 31:

The combination of Hokola and Vanderveen discloses the **method according to claim 18** as above, **wherein the key agreement procedure comprises: a three-pass authentication procedure; or a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.** (See Vanderveen [0079])

Examiner supplies the same rational for the combination of the reference as in claim 18 above.

17. Claims 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hokola and Vanderveen as applied to claim 18 as above; further in view of Ou (US 2009/0320102 A1), hereinafter Ou.

As for claim 28 and 29:

The combination of Hokola and Vanderveen teaches the **method according to claim 18** as above, neither Hokola nor Vanderveen discloses "**the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and wherein the verifying the validity of the initiation key is further based on the usage count."** However, Ou discloses the "usage" profile, the usage profile is "usage profile can indicate if the device has permission to create messages to send to the interest group". (See Ou [0028])

Ou, like Hokola and Vanderveen, is in the same field of endeavor of establish a peer-to peer communication session between the wireless communications (See Ou [0002]) discloses the “usage profile” with the access key.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to implement the teaching of Ou with the modified-invention of Hokola for a D2D communication session with mobile devices with “usage” profile that further enhance the security of the cellular communication network.

Claim 29, depends on claim 28, recites similar limitations to claim 28, mutatis mutandis, the subject matter of claim 29 which is therefore also considered to be taught by the combination of Hokola, Vanderveen and Ou as recited above.

Conclusion

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

A. US 20130054967 A1; Davoust et al; "Reoccuring Keying System";

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Taghi T Arani can be reached on (571)272-3787. 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.

/JASON LEE/

Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 14/424,691	Applicant(s)/Patent Under Reexamination NORP ET AL.	
	Examiner JASON LEE	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2013/0013926 A1	01-2013	Hakola; Sami-Jukka	H04W12/04	713/171
*	B	US-2013/0227655 A1	08-2013	Vanderveen; Michaela	H04L63/0823	726/4
*	C	US-2009/0320102 A1	12-2009	Ou; Shukong	H04L12/5895	726/4
*	D	US-2013/0054967 A1	02-2013	Davoust; Nancy	H04L63/20	713/168
	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	CPC 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.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14424691	NORP ET AL.
	Examiner	Art Unit
	JASON LEE	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
h04l63/061.cpci.;h04l63/062.cpci.	11/30/15	JL

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	4	11/28/15	JL
713	171	11/28/15	JL

SEARCH NOTES		
Search Notes	Date	Examiner
EAST searched, google patent searched	11/28/15	JL
inventer name and assignee searched	11/28/16	JL
"20090320102".pn. and (usage or count);("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (key same (validity with (time or period)));"20130013926".pn. and ((session) and generat$3);("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (mobile) and (device-to-device);h04l63/061.cpci.;h04l63/062.cpci.;(key same (usage with count));	11/28/15	JL

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

14424691 - GAU: 2438

Receipt date: 02/27/2015

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** February 27, 2015 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000		U.S. NATIONAL STAGE OF APPLICATION NO. PCT/EP2013/067904
	FIRST NAMED INVENTOR Antonius Norp		FILING DATE August 29, 2013
	EXAMINER Jason Lee	CONFIRMATION NO.	GROUP 2438

U.S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Number-Kind Code (if known)	ISSUE DATE / PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
/J.L./	1.	2007/0253376 A1	11-01-2007	Bonta, et al.
	2.			
	3.			
	4.			
	5.			
	6.			
	7.			
	8.			
	9.			
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			

Copies of issued U.S. Patents and Published U.S. Applications are not required and are not being provided. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.

EXAMINER	DATE CONSIDERED

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** February 27, 2015 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000		U.S. NATIONAL STAGE OF APPLICATION NO. PCT/EP2013/067904
	FIRST NAMED INVENTOR Antonius Norp		FILING DATE August 29, 2013
	EXAMINER Jason Lee	CONFIRMATION NO.	GROUP 2438

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Country Code-Number-Kind Code (if known)	DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
/J.L./	1.	WO 2010/030515 A2	03-18-2010	QUALCOMM Incorporated
/J.L./	2.	WO 2011/117677 A1	09-29-2011	Nokia, Inc.
	3.			
	4.			
	5.			
	6.			
	7.			
	8.			
	9.			
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			
	19.			
	20.			

EXAMINER	DATE CONSIDERED

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** February 27, 2015 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000		U.S. NATIONAL STAGE OF APPLICATION NO. PCT/EP2013/067904
	FIRST NAMED INVENTOR Antonius Norp		FILING DATE August 29, 2013
	EXAMINER Jason Lee	CONFIRMATION NO.	GROUP 2438

Examiner's Initials	Cite No.	**OTHER DOCUMENTS** *(Including Author, Title, Date, Pertinent Pages, Etc.)*
/J.L./	1.	Fodor, G., et al., "Design Aspects of Network Assisted Device-to-Device Communications," *IEEE Communications Magazine*, pp. 170-177, March 2012.
/J.L./	2.	Notification of Transmittal of The International Search Report and The Written Opinion of the International Searching Authority, PCT/EP2013/067904, date of mailing October 7, 2013.
	3.	
	4.	
	5.	
	6.	
	7.	
	8.	
	9.	
	10.	
	11.	
	12.	
	13.	
	14.	
	15.	
	16.	
	17.	
	18.	
	19.	

***Copies of any U.S. Office Communications or non-published U.S. Patent Applications are not being provided because the examiner has access to such documents through PAIR. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.**

EXAMINER /Jason Lee/	DATE CONSIDERED 11/28/2015

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	4	"20130013926".pn. or "20130227655".pn. and (disabl$3 or delet$3 or eras$3 or remov$3 or cancel$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:46
L4	4	"20130013926".pn. or "20130227655".pn. and (different or overlap$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:49
L5	2	("20130013926".pn. or "20130227655".pn.) and (different or overlap$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:49
L6	0	("20130013926".pn. or "20130227655".pn.) and (virtual)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:53
L7	1	("20130013926".pn. or "20130227655".pn.) and (virtual or identity)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:54
L8	0	("20130013926".pn. or "20130227655".pn.) and (count)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:58
L9	5	("20130013926".pn. or "20130227655".pn.) and (count or us$3 or limit$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 12:58
L10	1	("20130013926".pn. or "20130227655".pn.) and ((shared secret) or Diffie)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:11
L11	1	("20130013926".pn. or "20130227655".pn.) and ((shared	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/12/01 13:13

		secret) or Diffie or pass)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
L12	2	("20130013926".pn. or "20130227655".pn.) and ((request)same key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:15
L13	0	"20070253376".pn. and usage	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:22
L14	0	"20070253376".pn. and (usage or count)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:23
L15	1	"20090320102".pn. and (usage or count)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:24
L16	0	"20080095361".pn. and (usage or count)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 13:25
L17	0	h04l63/61.cpci.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:11
L18	6136	h04l63/061.cpci.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:11
L19	6838	h04l63/062.cpci.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:11
L20	354	18 and 19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:12
L21	301	20 and @ad < "20120906"	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/12/01 14:12

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
L22	0	21 and ((mobile) and (device-to-device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:13
L23	103	21 and ((mobile) or (device-to-device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:13
L24	7350	h04w76/023.cpci.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:14
L25	0	23 and 24	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:14
L26	0	21 and 24	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:15
L27	3271	24 and @ad <"20120906"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:15
L28	436	27 and (device-to-device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:16
L29	0	28 and (key with usage)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:16
L30	0	28 and (key same usage)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:17
L31	10	21 and (key same usage)	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/12/01 14:17

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
L32	0	21 and (key same2 (usage with count))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:20
L33	0	21 and (usage with count)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:20
L34	613	(key same (usage with count))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:21
L35	470	34 and @ad <"20120906"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:22
L36	8	35 and (18 or 19)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/12/01 14:23
S1	2	"20150222612".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 15:46
S2	2	"20070253376".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:02
S3	3	"20130013926".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:14
S4	0	"200800209440".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:19
S5	2	"20080209440".pn.	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/11/28 16:20

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S6	2	"20130227655".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:24
S7	0	"2009320102".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:30
S8	2	"20090320102".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:30
S9	3	"20080095361".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 16:31
S10	2	("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (mobile) and (device-to-device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:00
S11	2	("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (mobile) and (device-to-device) and key	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:14
S12	2	"20130013926".pn. and (key with value)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:18
S13	1	("20070253376".pn. or "20130227655".pn. or "20130013926".pn. or "20090320102".pn. or "20080095361".pn.) and (key same (validity with (time or period)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:23
S14	0	"20130013926".pn. and ((key with session) same generat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:35
S15	0	"20130013926".pn. and ((key with session) same2 generat$3)	US-PGPUB; USPAT; USOCR;	ADJ	ON	2015/11/28 17:35

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S16	0	"20130013926".pn. and ((key with session) and generat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:35
S17	1	"20130013926".pn. and ((session) and generat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/11/28 17:36

EAST Search History (Interference)

<This search history is empty>

12/ 1/ 2015 2:55:48 PM
C:\ Users\ jlee16\ Documents\ EAST\ Workspaces\ 14424691-112815.wsp

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. 1653

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/424,691	02/27/2015	726	2438	4965.1017-000

APPLICANTS

Koninklijke KPN N.V., The Hague, NETHERLANDS;
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO, Den Haag, NETHERLANDS;

INVENTORS

Antonius Norp, The Hague, NETHERLANDS;
Frank Fransen, Zuidhorn, NETHERLANDS;
Sander De Kievit, Leiden, NETHERLANDS;

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

This application is a 371 of PCT/EP2013/067904 08/29/2013

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

EUROPEAN PATENT OFFICE (EPO) 12183256.2 09/06/2012

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

04/27/2015

Foreign Priority claimed ☑ Yes ☐ No 35 USC 119(a-d) conditions met ☑ Yes ☐ No Verified and Acknowledged /JASON T LEE/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		NETHERLANDS	5	17	2

ADDRESS

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133
UNITED STATES

TITLE

Establishing A Device-To-Device Communication Session

FILING FEE RECEIVED		
1620	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
	14424691	NORP ET AL.
	Examiner	Art Unit
	JASON LEE	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/01/2015								
	1	-								
	2	-								
	3	-								
	4	-								
	5	-								
	6	-								
	7	-								
	8	-								
	9	-								
	10	-								
	11	-								
	12	-								
	13	-								
	14	-								
	15	-								
	16	-								
	17	-								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								

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
14/424,691	02/27/2015	Antonius Norp	4965.1017-000

CONFIRMATION NO. 1653

PUBLICATION NOTICE

21005
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

OC000000076723042

Title: Establishing A Device-To-Device Communication Session

Publication No.US-2015-0222612-A1
Publication Date:08/06/2015

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

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
14/424,691	02/27/2015	2431	1620	4965.1017-000	17	2

CONFIRMATION NO. 1653
CORRECTED FILING RECEIPT

21005
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

OC000000075272604

Date Mailed: 05/22/2015

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**

Inventor(s)

Antonius Norp, The Hague, NETHERLANDS;
Frank Fransen, Zuidhorn, NETHERLANDS;
Sander De Kievit, Leiden, NETHERLANDS;

Applicant(s)

Koninklijke KPN N.V., The Hague, NETHERLANDS;
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO, Den Haag, NETHERLANDS;

Power of Attorney: The patent practitioners associated with Customer Number 021005

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP2013/067904 08/29/2013

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) 12183256.2 09/06/2012

If Required, Foreign Filing License Granted: 04/27/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/424,691**

Projected Publication Date: 08/06/2015

Non-Publication Request: No

Early Publication Request: No

Title

Establishing A Device-To-Device Communication Session

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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).

SelectUSA

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 U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors:	Antonius Norp, Frank Fransen and Sander De Kievit		
Application No.:	14/424,691	Group:	Not yet assigned
Filed:	August 29, 2013	Examiner:	Not yet assigned

Confirmation No.: 1653

For: Establishing A Device-To-Device Communication Session

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or is being facsimile transmitted to the United States Patent and Trademark Office on:

_____ _____
Date Signature

_____
Typed or printed name of person signing certificate

REQUEST FOR CORRECTED FILING RECEIPT FOR NONPROVISIONAL APPLICATION

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

Commissioner:

We hereby request that the following items of information be corrected in the Filing Receipt received in this office on May 1, 2015 for the subject application.

A copy of a recently filed Application Data Sheet is submitted herewith.

The errors and corrections appear below.

In the Applicant(s) section please delete "Koninklijka" and insert ---Koninklijke---.

Enclosed are copies of the Filing Receipt with changes noted thereon and a copy of the Application Data Sheet.

We hereby request that the errors which are identified above be corrected in the captioned application to which this request for correction is directed. It is understood that the Patent Office will issue an automatically-generated, corrected Filing Receipt in this and, if applicable, any other affected applications.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By /Timothy J. Meagher, Reg. No. 39,302/
Timothy J. Meagher
Registration No. 39,302
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Date: 5/18/2015

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
14/424,691	02/27/2015		1620	4965.1017-000	17	2

CONFIRMATION NO. 1653

21005
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

FILING RECEIPT



TJM
Received
Hamilton Brook
Smith & Reynolds, P.C.,
By EDV on May 01, 2015

Date Mailed: 05/01/2015

Reviewed by: _____

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**

Inventor(s)

Antonius Norp, The Hague, NETHERLANDS;
Frank Fransen, Zuidhorn, NETHERLANDS;
Sander De Kievit, Leiden, NETHERLANDS;

Applicant(s)

Koninklijke ~~Koninklijka~~ KPN N.V., The Hague, NETHERLANDS
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO, Den Haag, NETHERLANDS

Power of Attorney: The patent practitioners associated with Customer Number 021005

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP2013/067904 08/29/2013

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) 12183256.2 09/06/2012

If Required, Foreign Filing License Granted: 04/27/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/424,691**

Projected Publication Date: 08/06/2015

Non-Publication Request: No

Early Publication Request: No

Title

Establishing A Device-To-Device Communication Session

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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).



SelectUSA

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 U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	

Title of Invention	Establishing A Device-To-Device Communication Session

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.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Antonius		Norp	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	The Hague	Country of Residence [i]	NL

Mailing Address of Inventor:

Address 1	Cornelis Jolstraat 83		
Address 2			
City	The Hague	State/Province	
Postal Code	NL-2584	Country [i]	NL

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Frank		Fransen	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Zuidhorn	Country of Residence [i]	NL

Mailing Address of Inventor:

Address 1	Brilweg 21		
Address 2			
City	Zuidhorn	State/Province	
Postal Code	NL-9801	Country [i]	NL

Inventor 3 Remove

Legal Name

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Sander		De Kievit	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Leiden	Country of Residence [i]	NL

Mailing Address of Inventor:

Address 1	Ravenhorst 61		
Address 2			
City	Leiden	**State/Province**	
Postal Code	NL-2317	**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.**

Customer Number	021005		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Establishing A Device-To-Device Communication Session		
Attorney Docket Number	4965.1017-000	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	5	**Suggested Figure for Publication (if any)**	1

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

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).
Either enter 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	021005		

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.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	a 371 of international	PCT/EP2013/067904	2013-08-29

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. 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(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)
12183256.2	EP	2012-09-06	

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

(●) Assignee	( ) Legal Representative under 35 U.S.C. 117	( ) Joint Inventor
( ) Person to whom the inventor is obligated to assign.	( ) Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	Koninklijke KPN N.V.		
Mailing Address Information For Applicant:			
Address 1	P.O. Box 95321		
Address 2			
City	The Hague	**State/Province**	
Country	NL	Postal Code	2509 CH
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Applicant 2

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

(●) Assignee	( ) Legal Representative under 35 U.S.C. 117	( ) Joint Inventor
( ) Person to whom the inventor is obligated to assign.	( ) Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

If the Applicant is an Organization check here. ☒			
Organization Name	Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO		
Mailing Address Information For Applicant:			
Address 1	Anna van Buerenplein 1		
Address 2			
City	Den Haag	**State/Province**	
Country i	NL	Postal Code	2595 DA
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

Signature:

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

Signature	/Timothy J. Meagher, Reg. No. 39302/			Date (YYYY-MM-DD)	2015-02-27
First Name	Timothy J.	Last Name	Meagher	Registration Number	39302

Additional Signature may be generated within this form by selecting the Add button.

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 C o o p eration 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:	22372795
Application Number:	14424691
International Application Number:	
Confirmation Number:	1653
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Customer Number:	21005
Filer:	Timothy J. Meagher/Julie Kertyzak
Filer Authorized By:	Timothy J. Meagher
Attorney Docket Number:	4965.1017-000
Receipt Date:	18-MAY-2015
Filing Date:	27-FEB-2015
Time Stamp:	14:12:22
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	49651017000ReqCorrFR.PDF	87719 da8d0576b9da7246d792cc3e364dddf0e3119dc3	no	5

Warnings:	
Information:	

2	Application Data Sheet	49651017000NewADS.PDF	114582 3e5f8d0267260ca5b9ac2ba63815d680989dee33	no	8

Warnings:	
Information:	
This is not an USPTO supplied ADS fillable form	
Total Files Size (in bytes):	202301

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

U.S. APPLICATION NUMBER NO.	FIRST NAMED INVENTOR	ATTY. DOCKET NO.
14/424,691	Antonius Norp	4965.1017-000

21005
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

INTERNATIONAL APPLICATION NO.	
PCT/EP2013/067904	
I.A. FILING DATE	PRIORITY DATE
08/29/2013	09/06/2012

CONFIRMATION NO. 1653
371 ACCEPTANCE LETTER

OC000000074850464

Date Mailed: 05/01/2015

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 ACCEPTED the above identified international application for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above. A Filing Receipt will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE "FILING DATE or 371(c) DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1) and (c)(2) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN BELOW.** 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)

02/27/2015
DATE OF RECEIPT OF 35 U.S.C.
371(c)(1) and (c)(2) REQUIREMENTS

The following items have been received:

- Copy of the International Application filed on 02/27/2015
- Copy of the International Search Report filed on 02/27/2015
- Preliminary Amendments filed on 02/27/2015
- Information Disclosure Statements filed on 02/27/2015
- Inventor's Oath or Declaration filed on 04/17/2015
- U.S. Basic National Fees filed on 02/27/2015
- Priority Documents filed on 02/27/2015
- Power of Attorney filed on 04/17/2015
- Application Data Sheet (37 CFR 1.76) filed on 02/27/2015

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)

BRIAN A HARDEN

Telephone: (703) 756-1815

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
14/424,691	02/27/2015		1620	4965.1017-000	17	2

CONFIRMATION NO. 1653

21005
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

FILING RECEIPT



Date Mailed: 05/01/2015

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**

Inventor(s)

Antonius Norp, The Hague, NETHERLANDS;
Frank Fransen, Zuidhorn, NETHERLANDS;
Sander De Kievit, Leiden, NETHERLANDS;

Applicant(s)

Koninklijka KPN N.V., The Hague, NETHERLANDS
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO, Den Haag, NETHERLANDS

Power of Attorney: The patent practitioners associated with Customer Number 021005

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP2013/067904 08/29/2013

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) 12183256.2 09/06/2012

If Required, Foreign Filing License Granted: 04/27/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/424,691**

Projected Publication Date: 08/06/2015

Non-Publication Request: No

Early Publication Request: No

Title

Establishing A Device-To-Device Communication Session

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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).

SelectUSA

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 U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/424,691

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	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	480
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	17 minus 20 =	*			OR	x 80 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 420 =	0.00
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).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
			TOTAL			TOTAL	1480

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

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.

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

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

Application Number	Filing Date
14424691	

Applicant(s) Antonius Norp

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

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

GENERAL POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

☒ I hereby appoint Practitioners associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

021005

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number		Name	Registration Number

Please recognize or change the correspondence address for the above-identified patent to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name:					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant and Assignee or Person to Whom the Inventor is Under an Obligation to Assign

A copy of this form, together with a transmittal letter (Form PTO/AIA/82A or equivalent) is required to be filed in each application in which this form is used. The transmittal letter may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Applicant for Patent

Signature		Date	28-04-2014
Name	Km Wright	Telephone	+31 70 3433955
Title	Corporate Intellectual Property Officer		
Company	Koninklijke KPN N.V.		

NOTE: See 37 CFR 1.4 for signature requirements and certifications.

1591247.v1

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

GENERAL POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

☒ I hereby appoint Practitioners associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

021005

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number		Name	Registration Number

Please recognize or change the correspondence address for the above-identified patent to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name:					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant and Assignee or Person to Whom the Inventor is Under an Obligation to Assign

A copy of this form, together with a transmittal letter (Form PTO/AIA/82A or equivalent) is required to be filed in each application in which this form is used. The transmittal letter may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Applicant for Patent

Signature		Date	11 April 2014
Name	Hendrik Pieter Drop	Telephone	+31 88 8668264
Title	Deputy Director Patents and Licensing TNO		
Company	Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO		

NOTE: See 37 CFR 1.4 for signature requirements and certifications.

1591248.v1

Electronic Acknowledgement Receipt

EFS ID:	22095036
Application Number:	14424691
International Application Number:	
Confirmation Number:	1653
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Customer Number:	21005
Filer:	Timothy J. Meagher/Julie Kertyzak
Filer Authorized By:	Timothy J. Meagher
Attorney Docket Number:	4965.1017-000
Receipt Date:	17-APR-2015
Filing Date:	
Time Stamp:	16:12:55
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	Transmittal Letter	49651017000TransDec.pdf	63951 389ee7adf89d171272e760db85060a228b7016f1	no	1

Warnings:	
Information:	

2	Oath or Declaration filed	49651017000Decs.PDF	211759 ea5e2b8eb6e064e246cb3e68f448ff70871f0dc3	no	3
Warnings:					
Information:					
3	Transmittal Letter	49651017000TransPOA.pdf	93113 d873af18afc7fff744f73cd76251e1365d65f055	no	1
Warnings:					
Information:					
4	Power of Attorney	49651017000POAs.PDF	124072 683c93559265b9c6977dc325c81c2722c653d9ef	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	492895		

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

Inventors: Antonius Norp, Frank Fransen and Sander De Kievit

Application No.: 14/424,691 Group: Not Yet Assigned

Filed: August 29, 2013 Examiner: Not Yet Assigned

Confirmation No.: 1653

For: Establishing A Device-To-Device Communication Session

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450, or is being facsimile transmitted to the United States Patent and Trademark Office on:

Date Signature

Typed or printed name of person signing certificate

TRANSMITTAL OF DECLARATION

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

Commissioner:

Enclosed are executed Declarations for filing in the above identified application.

The surcharge for late filing of the enclosed Declaration in the amount of $140 was previously charged to Deposit Account 08-0380, concurrently with the application filing fees, paid on February 27, 2015.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By /Timothy J. Meagher, Reg. No. 39,302/
Timothy J. Meagher
Registration No.: 39,302
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Date: 4/17/2015

DOCKET NO. 4965.1017-000

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Establishing A Device-To-Device Communication Session

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/424,691 filed on August 29, 2013.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims.

I acknowledge the duty to disclose to the Patent Office all information known to me to be 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.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Antonius Norp

Date (Optional): April 2015

Signature:

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 (or equivalent) form for each additional inventor.

1804506 v1

DOCKET NO. 4965.1017-000

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Establishing A Device-To-Device Communication Session

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/424,691 filed on August 29, 2013.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims.

I acknowledge the duty to disclose to the Patent Office all information known to me to be 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.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Frank Fransen Date (Optional): 10 April 2015

Signature:

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 (or equivalent) form for each additional inventor.

1804506 v1

DOCKET NO. 4965.1017-000

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Establishing A Device-To-Device Communication Session

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/424,691 filed on August 29, 2013.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims.

I acknowledge the duty to disclose to the Patent Office all information known to me to be 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.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Sander De Kievit

Date (Optional): 30-March-2015

Signature: 

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 (or equivalent) form for each additional inventor.

1804506.v1

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B or equivalent) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5. If the Power of Attorney by Applicant form is not accompanied by this transmittal form or an equivalent, the Power of Attorney will not be recognized in the application.

Application Number	14/424,691
Filing Date	August 29, 2013
First Named Inventor	Antonius Norp
Title	Establishing A Device-To-Device Communication Session
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	4965.1017-000

SIGNATURE of Applicant or Patent Practitioner

Signature	/Timothy J. Meagher, Reg. No. 39,302/	Date	4/17/2015
Name	Timothy J. Meagher	Telephone	(978) 341-0036
Registration Number	39,302		

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

☒ *Total of 2 forms are submitted.

PCT REQUEST

Print Out (Original in Electronic Form)

0	**For receiving Office use only**	
0-1	International Application No.	**PCT/EP2013/067904**
0-2	International Filing Date	**29 AUG 2013 (29.08.2013)**
0-3	Name of receiving Office and "PCT International Application"	**RO/EP**

0-4	**Form PCT/RO/101 PCT Request**	
0-4-1	Prepared Using	PCT Online Filing Version 3.5.000.235 MT/FOP 20020701/0.20.5.20
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	European Patent Office (EPO) (RO/EP)
0-7	**Applicant's or agent's file reference**	403638WO
I	**Title of Invention**	ESTABLISHING A DEVICE-TO-DEVICE COMMUNICATION SESSION
II	**Applicant**	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States
II-4	Name	KONINKLIJKE KPN N.V.
II-5	Address	Maanplein 55 2516 CK The Hague Netherlands
II-6	State of nationality	NL
II-7	State of residence	NL
II-8	Telephone No.	+31 70 343 39 55
II-9	Facsimile No.	+31 70 385 54 37
II-10	e-mail	dieneke.vandertoorn-dejager@kpn.com
III-1	**Applicant and/or inventor**	
III-1-1	This person is	Applicant only
III-1-2	Applicant for	All designated States
III-1-4	Name	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO
III-1-5	Address	Schoemakerstraat 97 2628 VK Delft Netherlands
III-1-6	State of nationality	NL
III-1-7	State of residence	NL

PCT REQUEST

Print Out (Original in Electronic Form)

III-2	**Applicant and/or inventor**	
III-2-1	This person is	Inventor only
III-2-3	Inventor for	
III-2-4	Name (LAST, First)	NORP, Antonius
III-2-5	Address	Cornelis Jolstraat 83 2584 EN The Hague Netherlands
III-3	**Applicant and/or inventor**	
III-3-1	This person is	Inventor only
III-3-3	Inventor for	
III-3-4	Name (LAST, First)	FRANSEN, Frank
III-3-5	Address	Brilweg 21 9801 GC Zuidhorn Netherlands
III-4	**Applicant and/or inventor**	
III-4-1	This person is	Inventor only
III-4-3	Inventor for	
III-4-4	Name (LAST, First)	DE KIEVIT, Sander
III-4-5	Address	Ravenhorst 61 2317 AG Leiden Netherlands
IV-1	**Agent or common representative; or address for correspondence**	
	The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent
IV-1-1	Name (LAST, First)	WUYTS, Koenraad
IV-1-2	Address	P.O. Box 95321 2509 CH The Hague Netherlands
IV-1-3	Telephone No.	+31 70 343 39 55
IV-1-4	Facsimile No.	+31 70 385 54 37
IV-1-5	e-mail	dieneke.vandertoorn-dejager@kpn.com
V	**DESIGNATIONS**	
V-1	**The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.**	
VI-1	**Priority claim of earlier regional application**	
VI-1-1	Filing date	06 September 2012 (06.09.2012)
VI-1-2	Number	12183256.2
VI-1-3	Regional Office	EP

PCT REQUEST

Print Out (Original in Electronic Form)

VI-2	**Priority document request** The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1	
VI-3	**Incorporation by reference :** where an element of the international application referred to in Article 11(1)(iii)(d) or (e) or a part of the description, claims or drawings referred to in Rule 20.5(a) is not otherwise contained in this international application but is completely contained in an earlier application whose priority is claimed on the date on which one or more elements referred to in Article 11(1)(iii) were first received by the receiving Office, that element or part is, subject to confirmation under Rule 20.6, incorporated by reference in this international application for the purposes of Rule 20.6.		
VII-1	**International Searching Authority Chosen**	European Patent Office (EPO) (ISA/EP)	
VII-2	**Request to use results of earlier search; reference to that search**		
VII-2-1	Filing date	06 September 2012 (06.09.2012)	
VII-2-2	Application Number	12183256.2	
VII-2-3	Country (or regional Office)	EP	
VII-2-5	Documents are available to the ISA in a form and manner acceptable to it and therefore do not need to be submitted by the applicant to the ISA (Rule 12bis.1(f)):	A copy of the results of the earlier search A copy of the earlier application A copy of any document cited in the results of the earlier search	
VIII	**Declarations**	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	-	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	-	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	-	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	1	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	-	

PCT REQUEST

Print Out (Original in Electronic Form)

IX	Check list	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	6	✓
IX-2	Description	22	✓
IX-3	Claims	4	✓
IX-4	Abstract	1	✓
IX-5	Drawings	5	✓
IX-7	TOTAL	38	
	Accompanying Items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	–	✓
IX-18	PCT-SAFE physical media	–	–
IX-20	**Figure of the drawings which should accompany the abstract**	1	
IX-21	**Language of filing of the international application**	English	
X-1	**Signature of applicant, agent or common representative**	(PKCS7 Digital Signature)	
X-1-1	Name (LAST, First)	WUYTS, Koenraad	
X-1-2	Name of signatory	NL, Koninklijke KPN N.V., K. Wuyts 16870	
X-1-3	Capacity (if such capacity is not obvious from reading the request)	(Representative)	

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	**29 AUG 2013 (29.08.2013)**
10-2	**Drawings:**	
10-2-1	Received ✓	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/EP
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92*bis*.1 and Administrative Instructions, Section 422)

To:

WUYTS, Koenraad
P.O. Box 95321
NL-2509 CH The Hague
PAYS-BAS

Date of mailing *(day/month/year)*
24 February 2015 (24.02.2015)

Applicant's or agent's file reference
403638WO

IMPORTANT NOTIFICATION

International application No.
PCT/EP2013/067904

International filing date *(day/month/year)*
29 August 2013 (29.08.2013)

1. The following indications appeared on record concerning:

☒ the applicant ☐ the inventor ☐ the agent ☐ the common representative

Name and Address
NEDERLANDSE ORGANISATIE VOOR
TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO
Schoemakerstraat 97
NL-2628 VK Delft
Netherlands

State of Nationality: NL
State of Residence: NL
Telephone No.
Facsimile No.
E-mail address

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☒ the address ☐ the nationality ☐ the residence

Name and Address
NEDERLANDSE ORGANISATIE VOOR
TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK TNO
Anna van Buerenplein 1
NL-2595 DA The Hague
Netherlands

State of Nationality: NL
State of Residence: NL
Telephone No.
Facsimile No.
E-mail address
☐ Notifications by e-mail authorized

3. Further observations, if necessary:
The change takes place as from March, 1st 2015.

4. A copy of this notification has been sent to:

☒ the receiving Office
☐ the International Searching Authority
☐ the Authority(ies) specified for supplementary search
☐ the International Preliminary Examining Authority
☒ the designated Offices concerned
☐ the elected Offices concerned
☐ other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 89 75

Authorized officer
Bouvier Alexandre
e-mail pt05.pct@wipo.int
Telephone No. +41 22 338 74 05

PCT REQUEST

Print Out (Original in Electronic Form)

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 inventor or an original joint inventor of a claimed invention in the application. This declaration is directed to the international application of which it forms a part. I hereby declare that the above-identified international application was made or authorized to be made by me. I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.
VIII-4-1-1-1	Name (LAST, First)	NORP, Antonius
VIII-4-1-1-2	Residence: (city and either US state, if applicable, or country)	The Hague, Netherlands
VIII-4-1-1-3	Mailing Address:	Cornelis Jolstraat 83 2584 EN The Hague Netherlands
VIII-4-1-1-4	Inventor's Signature: (The signature must be that of the inventor, not that of the agent)	/Toon Norp/
VIII-4-1-1-5	Date:	27 August 2013 (27.08.2013)
VIII-4-1-2-1	Name (LAST, First)	FRANSEN, Frank
VIII-4-1-2-2	Residence: (city and either US state, if applicable, or country)	Zuidhorn, Netherlands
VIII-4-1-2-3	Mailing Address:	Brilweg 21 9801 GC Zuidhorn Netherlands
VIII-4-1-2-4	Inventor's Signature: (The signature must be that of the inventor, not that of the agent)	/Frank Fransen/
VIII-4-1-2-5	Date:	27 August 2013 (27.08.2013)

PCT REQUEST

Print Out (Original in Electronic Form)

VIII-4-1-3-1	Name (LAST, First)	DE KIEVIT, Sander
VIII-4-1-3-2	Residence: (city and either US state, if applicable, or country)	Leiden, Netherlands
VIII-4-1-3-3	Mailing Address:	Ravenhorst 61 2317 AG Leiden Netherlands
VIII-4-1-3-4	Inventor's Signature: (The signature must be that of the inventor, not that of the agent)	/Sander de Kievit/
VIII-4-1-3-5	Date:	27 August 2013 (27.08.2013)

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°**

12183256.2 / EP12183256

The organization code and number of your priority application, to be used for filing abroad under the Paris Convention, is EP12183256.

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.

U. Ingmann

Anmeldung Nr:
Application no.: 12183256.2
Demande no :

Anmeldetag:
Date of filing: 06.09.12
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, oder falls die Anmeldung in einer Nicht-Amtssprache des EPA eingereicht wurde, siehe Beschreibung bezüglich ursprünglicher Bezeichnung.
If no title is shown, or if the application has been filed in a non-EPO language, please refer to the description for the original title.
Si aucun titre n'est indiqué, ou si la demande a été déposée dans une langue autre qu'une langue officielle de l'OEB, se référer à la description pour le titre original.)

Establishing a device-to-device communication session

In Anspruch genommene Priorität(en) / Priority(Priorities) claimed / Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen / State/Date/File no. / Pays/Date/Numéro de dépôt:

Am Anmeldetag benannte Vertragstaaten / Contracting States designated at date of filing / Etats contractants désignées lors du dépôt:

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Establishing a device-to-device communication session

FIELD OF THE INVENTION

The invention relates to a method for establishing a device-to-device (D2D) communication session between mobile devices. The invention further relates to a mobile device for establishing the D2D communication session with a further mobile device. The invention further relates to control software comprising instructions for execution on the mobile device. The invention further relates to the mobile network.

Mobile communication networks, also referred to as cellular networks or mobile networks, have been extensively deployed over the last decades in order to address the increasing need for mobile communication. Communication between mobile devices which are connected to such a mobile network typically takes place via the mobile network, i.e., via one or more base stations and core nodes of the mobile network.

BACKGROUND OF THE INVENTION

It is desirable to enable mobile devices which are typically connected to a mobile network to also directly communicate with each other, i.e., via so-termed device-to-device (D2D) communication.

D2D communication is characterized by a direct wireless communication path between two mobile terminals, such as the mobile devices, while maintaining, at least at some moments in time, at least a signaling connection with/via a base station of the wireless communication network, i.e., of the mobile network. The direct wireless communication path between mobile terminals allows to offload the base station(s), the access network and the core network of the wireless communication network from most of the data and signaling exchanged between the mobile terminals. The signaling connection with (a base station of) the wireless communication network allows the wireless communication network to control the resources assigned to the direct communication path between the terminals.

A mobile device which, at a given time, uses D2D communication instead of communicating via the mobile network may be referred to as operating in Direct Mode Operation (DMO). DMO offers advantages such as, e.g., enabling mobile communication

between users outside a range of the mobile network, reducing of load from the base stations and/or from the core nodes of the mobile network, etc.

An example of a mobile communication standard which enables mobile communication between mobile devices both via the mobile network as well as via the aforementioned D2D communication is Terrestrial Trunked Radio (TETRA).

Another example of such a mobile communication standard is Global System for Mobile Communications (GSM). The GSM standard includes a so-termed local call, local switch feature in which mobile communication between mobile devices which are connected to a same base station of the mobile network is not routed through the core nodes of the mobile network, but rather directly from the base station to each respective mobile device.

Yet another example is Long Term Evolution (LTE). Recent developments in LTE include D2D communication between mobile devices. It is noted that in the context of LTE, such D2D communication is also referred to as Direct LTE.

SUMMARY OF THE INVENTION

A problem of the above mobile networks and mobile devices is that an operator of the mobile network has no or only limited control over the D2D communication. The inventors have recognized that such control is desirable for various reasons. For example, the D2D communication may take place in a frequency spectrum which is licensed to the operator and thus needs to be managed by the operator, e.g., to avoid interference. Another example is that the operator may desire to only grant specific users access to the D2D communication, e.g., emergency workers, subscribers to a D2D service, etc.

It would be advantageous to provide more control over the D2D communication between mobile devices which are connectable to a mobile network.

To better address this concern, a first aspect of the invention provides a method for establishing a D2D communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:

- preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and

on each of the mobile devices:

- verifying a validity of the initiation key based on a current time;
- if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between

the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and

- establishing the D2D communication session over the D2D communication channel based on the session key.

A further aspect of the invention provides control software comprising instructions for, upon execution of the control software on a mobile device, causing the mobile device to establish the D2D communication session according to the method set forth.

A further aspect of the invention provides a mobile device for establishing a D2D communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:

- a storage area for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and
- a computing subsystem for:
  - verifying a validity of the initiation key based on a current time;
  - if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device and the further mobile device matches; and
  - a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

A further aspect of the invention provides a mobile network arranged for preloading an initiation key on the mobile device set forth when the mobile device is connected to the mobile network, the initiation key being associated with a validity period.

The aforementioned measures establish, or provide the means to establish a D2D communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network. Here, the term communication channel refers to a conduit for an information exchange between the mobile devices, and the term communication session refers to the information interchange, with the information interchange typically having a defined start and end.

The mobile devices are connectable to the mobile network in that, when the mobile devices are connected to the mobile network, mobile communication between the mobile devices can take place via the mobile network, e.g., via the base stations and the core nodes of the mobile network. The mobile devices are also arranged for establishing a D2D communication channel between the mobile devices so as to enable direct communication. The D2D communication may be established between two mobile devices. However, the D2D communication may equally involve a plurality of more than two mobile devices.

The D2D communication session is established, i.e., set up, in the following manner. First, an initiation key is preloaded on each of the mobile devices. Here, the term preloading refers to a loading of the initiation key on a mobile device before establishing the D2D communication session. For example, the initiation key may be loaded on the mobile device already before a request is received to establish the D2D communication session. The initiation key is used on each of the mobile devices in establishing the D2D communication session. Hence, when a request for establishing the D2D communication session is received, e.g., from the user or another mobile device, it is not necessary anymore to obtain the initiation key in order to establish the D2D communication session, i.e., it is already available on the mobile device.

The initiation key is used in establishing the D2D communication session in the following ways. The initiation key is associated with a validity period. The validity period is available to the mobile device, e.g., by being provided next to the initiation key, being derivable from the initiation key, etc. The validity period indicates a period in time in which the initiation key is deemed to be valid for use in establishing the D2D communication session. On each of the mobile devices which are to take part in the D2D communication session, a validity of the initiation key is verified based on the current time. This may be in response to a request to establish the D2D communication session. The current time is thus used to determine whether the initiation key is considered to be valid or not. If the initiation key is considered to be valid, e.g., due to the current time being in the validity period, the initiation key is used in performing a key agreement procedure between the mobile devices.

Here, the term key agreement procedure refers to a procedure which is performed between the mobile devices which results in a session key being agreed on, with the mobile devices each being able to influence the outcome of the procedure, i.e., the session key. The key agreement procedure is performed via the D2D communication channel, e.g., by exchanging messages between the mobile devices, with the messages together constituting

the key agreement procedure. The messages may be exchanged as part of an initial D2D communication session having been established over the D2D communication channel.

The key agreement procedure provides the session key based on whether the initiation key, as used by each respective mobile device in the key agreement procedure, matches. As such, a valid session key is obtained provided that each respective mobile device uses a same initiation key in the key agreement procedure. The session key constitutes a key used for cryptographically protecting messages in a communication session, such as confidentiality protection using encryption or integrity protection using message authentication codes. The D2D communication session is established using the session key. Thus, a D2D communication session is obtained in which messages, such as those of a voice or video transmission between the mobile devices, are cryptographically protected using the session key. The session key is used for a particular D2D communication session. Hence, in order to establish a new D2D communication session at a later moment in time, typically a new session key needs to be obtained or generated.

The above measures have the effect that a D2D communication session is established based on an initiation key. Here, the initiation key essentially functions as an authorization token in that a mobile device needs the initiation key to establish the D2D communication session. By providing an initiation key which is associated with a validity period and verifying the validity of the initiation key on the mobile device based on a current time, a time-based control mechanism is provided in that the initiation key is deemed valid only in a predetermined period and deemed invalid outside of said period.

The above measures offer control to the operator over the D2D communication in the following ways. By requiring a valid initiation key to establish the D2D communication session, the operator obtains control in that he can chose to whom the initiation key is provided, according to which conditions, etc. Moreover, by means of the validity period, the operator obtains time-based control, e.g., so as to prevent the re-use of old initiation keys. By using the initiation key in a key agreement procedure which is based on a match of the initiation keys used by the mobile devices, the operator obtains control in that not just any initiation key can be used in establishing the D2D communication session; rather, a success of the key agreement procedure depends on whether the initiation key, as used by each of the mobile devices in establishing the D2D communication session, matches.

Advantageously, by preloading the initiation key, the D2D communication session can be established under the operator's control even when one or more of the mobile devices are currently outside the operator's direct control, e.g., by being outside a range of

the mobile network. Advantageously, the mobile devices can autonomously establish the D2D communication session, i.e., without a need for contacting 3rd parties.

Optionally, the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network. Preloading the initiation key via the mobile network is convenient as mobile devices are frequently connected to the mobile network and thus no additional means is needed for preloading the initiation key. Advantageously, the mobile network provides a secure channel for preloading the initiation key. Advantageously, the initiation key can be automatically preloaded, i.e., without requiring user actions.

Optionally, the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device. The initiation key is thus stored such that it cannot be easily read by, e.g., the user or an application running on the mobile device. Advantageously, a tampering with the initiation key is made more difficult.

Optionally, the secure storage area is provided by a trusted computing subsystem of each respective mobile device. Here, the mobile device comprises, either as an integral part or as a removable part, a trusted computing subsystem. Such a trusted computing subsystem may be used for performing computing steps on the mobile device which require a certain level of security, such as authenticating the mobile device on the mobile network. An example of a removable trusted computing subsystem is a so-termed Universal Integrated Circuit Card (UICC) which may, in turn, comprise a Universal Subscriber Identity Module (USIM) application for use in authenticating the mobile device on the mobile network. The secure storage area provided by such a trusted computing subsystem, e.g., the memory of the UICC, is well suited for securely storing the initiation key on the mobile device.

Optionally, at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem. Hence, the use of the initiation key outside of the secure storage area provided by the trusted computing subsystem is reduced or avoided. Advantageously, a tampering with the initiation key is made more difficult.

Optionally, the method further comprises:

- preloading a set of initiation keys on each of the mobile devices, the set of initiation keys key being associated with a respective set of validity periods; and
- performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.

As such, each of the mobile devices is provided with multiple different initiation keys. To enable a same initiation key being used by each of the mobile devices in establishing the D2D communication session, a key synchronization procedure is performed in which it is identified which initiation key is available to all or most of the mobile devices, with said initiation key being selected for use in establishing the D2D communication session. Advantageously, a suitable initiation key can be conveniently established. Advantageously, the key synchronization procedure provides feedback if a mobile device does not have a suitable initiation key before performing the key agreement procedure.

Optionally, the method further comprises:

- preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys; and
- performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.

By performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers, it is not needed to involve the initiation keys themselves in the key synchronization procedure, e.g., by exchanging the initiation keys over the D2D communication channel. Advantageously, a tampering with the initiation keys is made more difficult since only the key identifiers are exchanged. Nevertheless, a tampering of the key identifiers, e.g., so as to feign a matching of initiation keys, will still fail as the key agreement procedure only provides the session key if the actual initiation keys match.

Optionally, the method further comprises disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session. Thus, an initiation key can only be used once in establishing a D2D communication session. For establishing a new D2D communication session, a new initiation key is needed. Advantageously, the operator obtains control over a number of times that a D2D communication session can be established, e.g., for limiting said number of times.

Optionally, the set of validity periods is constituted at least in part by different but overlapping validity periods. The different but overlapping validity periods together constitute a larger period in time. Since the validity periods overlap, there are no gaps in the larger period in time. The different but overlapping validity periods are associated with initiation keys. As a result, at any point in time in the larger period, an initiation key is available that can be validly used in establishing the D2D communication session.

Optionally, the initiation key is associated with a virtual network identity, and the verifying the validity of the initiation key further comprises determining a match of the

virtual network identity on each of the mobile devices via the D2D communication channel. Thus, the D2D communication session can only be established between mobile devices that have a same virtual network identity. Advantageously, the operator can set up a virtual network of mobile devices between which D2D communication is possible, while preventing D2D communication with mobile devices outside of said virtual network or between mobile devices belonging to different virtual networks.

Optionally, the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and the verifying the validity of the initiation key is further based on the usage count. Advantageously, the operator obtains control over a number of times that a D2D communication session can be established. Advantageously, said control can be provided with one initiation key, e.g., a master key, which can be used for establishing multiple D2D communication sessions. Thus, it is not needed to provide a set of initiation keys which each can only be used once for establishing a D2D communication session.

Optionally, the method further comprises adjusting the usage count after use of the initiation key in establishing the D2D communication session. Hence, a use of the initiation key in establishing a D2D communication session is reflected in the usage count.

Optionally, the method further comprises requesting a further initiation key via the mobile network if i) no initiation key is deemed valid, or ii) the key agreement procedure fails in providing the session key.

Optionally, the key agreement procedure comprises:

- a three-pass authentication procedure; or
- a use of the initiation key to encrypt a message exchange

between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.

Modifications and variations of the control software, the mobile device and the mobile network, which correspond to the described modifications and variations of the method, can be carried out by a person skilled in the art based on the present description.

The invention is defined in the independent claims. Advantageous yet optional embodiments are defined in the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter. In the drawings,

Fig. 1 shows mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network;

Fig. 2 shows a method for establishing a D2D communication session between the mobile devices;

Fig. 3 shows a mobile device comprising a mobile subsystem and a computing subsystem, the computing subsystem comprising a storage area;

Fig. 4 shows a determining a match of a virtual network identity on each of the mobile devices via the D2D communication channel;

Fig. 5 shows a performing a key synchronization procedure between the mobile devices over the D2D communication channel;

Fig. 6 shows a key agreement procedure being initialized over the D2D communication channel by using an initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret;

Fig. 7 shows a key agreement procedure being performed over the D2D communication channel, being based on a three-pass authentication procedure; and

Fig. 8 shows another key agreement procedure being performed over the D2D communication channel in which identifiers identifying the mobile devices are encrypted.

It should be noted that items which have the same reference numbers in different Figures, have the same structural features and the same functions, or are the same signals. Where the function and/or structure of such an item has been explained, there is no necessity for repeated explanation thereof in the detailed description.

DETAILED DESCRIPTION OF EMBODIMENTS

Fig. 1 shows a first mobile device MD1 and a second mobile device MD2, henceforth also jointly referred to as mobile devices MD. The mobile devices MD are individually connectable to a mobile network MN. This is illustrated in Fig. 1 by a communication channel existing between each mobile device MD and the mobile network MN, i.e., a device-to-network communication channel DNC. The mobile network MN is shown to comprise base-stations BS1, BS2. In this particular example, each of the mobile devices MD is connected to a different one of the base-station BS1, BS2. The base-stations BS1, BS2 are mutually connected via core nodes CN of the mobile network. As such, when the mobile devices MD are connected to the mobile network MN, communication between the mobile devices MD can take place via the mobile network MN in that an information

interchange can be performed via a first one of the base-stations BS1, the core nodes CN, and a second one of the base-stations BS2 of the mobile network MN, or vice versa.

The mobile devices MD are also mutually connectable via a D2D communication channel DDC. The D2D communication channel DDC may have been established or setup using a mobile subsystem MS1, MS2 of each respective mobile device MD1, MD2. The present invention involves establishing a D2D communication session between the mobile devices MD over the D2D communication channel DDC.

The D2D communication session may be established in accordance with the method 100 as shown in Fig. 2. The method 100 comprises firstly preloading 120 an initiation key on each of the mobile devices MD. The preloading 120 may be performed using the mobile network MN. For that purpose, the mobile network MN may be arranged for, when one of the mobile devices MD is connected to the mobile network MN, providing the initiation key to said mobile device MD via the device-to-network communication channel DNC. However, the preloading 120 may also involve another communication channel, and in particular a secure communication channel. For example, the initiation key may be preloaded using Near Field Communication (NFC), e.g., at a physical point of sale, or using Wi-Fi, e.g., via a Wireless Local Area Network (WLAN).

Although not shown in Fig. 1, each mobile device MD may comprise a storage area for storing the initiation key on the respective mobile device MD. Consequently, the step of preloading 120 the initiation key on each of the mobile devices MD may comprise storing the initiation key in the storage area of the respective mobile device MD.

The initiation key is associated with a validity period. The method 100 further comprises, on each of the mobile devices MD, verifying 140 a validity of the initiation key based on a current time. For that purpose, each mobile device MD1, MD2 comprises a computing subsystem CS1, CS2 which is arranged for performing said step and which may have knowledge of the current time or be arranged for obtaining the current time. It is noted that the validity period may be expressed in any suitable time-based quantity, e.g., a day, an hour of a day, a minute of an hour, etc. Consequently, the term current time may refer to, e.g., a current day and/or a current time of the day. Hence, verifying the validity of the initiation key may comprise determining whether the current day falls within the validity period, and if so, whether the current day is either a first day or a last day of the validity period, and if so, whether the current time of the day falls within the validity period.

The method 100 further comprises, on each of the mobile devices MD, if the initiation key is deemed valid, generating 160 a session key using the initiation key by using

the initiation key in performing a key agreement procedure between the mobile devices MD over the D2D communication channel DDC. The computing subsystem CS1, CS2 of each mobile device MD is arranged for performing said step, while involving the mobile subsystem MS1, MS2 to carry out an actual message exchange over the D2D communication channel DDC.

The key agreement procedure is arranged for resulting in the session key if the initiation key used by each of the mobile devices MD matches. Having obtained the session key, the method 100 comprises, on each of the mobile devices MD, establishing 180 the D2D communication session over the D2D communication channel DDC based on the session key. The mobile subsystem MS1, MS2 of each mobile device MD is arranged for performing said step using the session key obtained from the computing subsystem CS1, CS2.

Although not shown in Fig. 2, control software may be provided comprising instructions for, upon execution of the control software on a mobile device, causing the mobile device to establish the D2D communication session according to the method 100 as shown in Fig. 2, i.e., by verifying 140 a validity of the initiation key based on a current time, generating 160 a session key using the initiation key, and establishing 180 the D2D communication session over the D2D communication channel based on the session key.

Fig. 3 shows the first mobile device MD1 in more detail, with the first mobile device MD1 here being exemplary of each of the mobile devices MD. The first mobile device MD1 comprises a mobile subsystem MS1 and a computing subsystem CS1 as introduced earlier in reference to Figs. 1 and 2. Here, the term mobile subsystem refers to a subsystem of the mobile device that performs and/or enables the main functionality of the mobile device, including establishing a communication channel, exchanging messages over the established communication channel, performing various computing functions, etc. An example of a mobile subsystem is a mobile System on a Chip (SoC) comprising an application processor, a display processor, one or more modems, an integrated LTE radio. Another example is said mobile SoC and an external LTE radio which is connected to the mobile SoC.

Fig. 3 shows the first mobile device MD1 comprising a storage area SA1 for storing the initiation key as provided during the preloading procedure. The storage area SA1 may be a secure storage area. In the example of Fig. 3, the storage area SA1 is provided by the computing subsystem CS1. The computing subsystem CS1 may be a trusted computing subsystem, thereby automatically providing a secure storage area. Such a trusted computing subsystem CS1 may be constituted by a UICC which comprises a USIM application. The USIM application may be arranged for establish the D2D communication session according

to the method 100 as shown in Fig. 2. The interface to and from the UICC may be protected by means of secure channel protocol, e.g., according to the ETSI TS 102 484 technical specification, so as to make eavesdropping and tampering more difficult.

In the following, two detailed embodiment of the present invention are presented which each comprise various advantageous yet optional measures. It will be appreciated that those measures may also be combined and/or individually applied to the general concept of the present invention, unless prevented by technical incompatibilities.

The first detailed embodiment comprises preloading a set of initiation keys on each of the mobile devices MD, the set of initiation keys key being associated with a respective set of validity periods. For that purpose, the mobile network MN may send one or more messages to the computing subsystem CS1, CS2 of each mobile device MD1, MD2 via each respective mobile subsystem MS1, MS2. The one or more messages may comprise the set of initiation keys and the set of validity periods. In addition, the one or more messages may comprise a current network time and/or a set of limitations. In addition to the set of initiation keys and the set of validity periods, the one or messages may comprise a set of key identifiers, each of the set of key identifiers identifying a respective one of the set of initiation keys. In addition to the set of initiation keys and the set of validity periods, the one or more messages may comprise a set of virtual network identities, each of the set of virtual network identities being associated with a respective one of the set of initiation keys.

The following table shows an example of the information which may be preloaded on a mobile device:

Virtual Network Id	**Key Id**	**Initiation key**	**Valid from (hh:mm dd:mm:yyyy)**	**Valid Through (hh:mm dd:mm:yyyy)**
Corporation X	102	Secret123	11:00 01/01/2012	13:00 02/01/2012
Corporation X	103	Geheim123	11:00 01/01/2012	13:00 02/01/2012
Corporation X	104	gEHEIM321	11:00 01/01/2012	13:00 02/01/2012
Corporation X	105	SeCRet123	11:00 02/01/2012	13:00 03/01/2012
Corporation X	106	GeHEim123	11:00 02/01/2012	13:00 03/01/2012
Corporation X	107	sEcrET321	11:00 02/01/2012	13:00 03/01/2012
Operator Y	53	sECRET321	00:00 01/12/2011	03:00 01/01/2012
Operator Y	54	123secret	00:00 01/12/2011	03:00 01/01/2012

Operator Y	55	sECRet321	00:00 01/01/2012	03:00 01/02/2012
Operator Y	56	123seCRet	00:00 01/01/2012	03:00 01/02/2012

In general, as is the case in the above example, the set of validity periods may be constituted at least in part by different but overlapping validity periods.

Each computing subsystem CS1, CS2 may store the set of initiation keys, the set of key identifiers and the current network time in a secure storage area SA1 of the computing subsystem. Each computing subsystem CS1, CS2 may also dispose of any initiation keys already stored which have expired according to the current network time. The set of virtual network identities may be stored elsewhere in each of the mobile devices MD1, MD2, i.e., may not need to be stored in the computing subsystem CS1, CS2.

As part of establishing the D2D communication session over the D2D communication channel DDC, it may be determined whether a virtual network identity on each of the mobile devices MD matches. This allows enabling D2D communication sessions to be established between mobile devices MD which share a virtual network identity, whilst preventing D2D communication sessions from being established between mobile devices MD which do not share a virtual network identity. For example, a corporate mobile device may comprise a virtual network identity of the corporation as well as a virtual network identity of the operator's own virtual network. The latter may allow users to establish a D2D communication session with other users of the operator's mobile network. In general, virtual network identities may be provided for, e.g., a certain locality, certain group of users, companies, families, etc. A virtual network identity may also be provided that allows cross-operator D2D communication sessions to be established, i.e., between mobile devices which normally belong to mobile networks that are operated by different operators.

Fig. 4 shows an example 142 of how a match of a virtual network identity on each of the mobile devices MD may be determined via the D2D communication channel DDC. Here, the computing subsystem CS1 and mobile subsystem MS1 of the first mobile device MD1 are schematically shown on a left-hand side, and the computing subsystem CS2 and mobile subsystem MS2 of the second mobile device MD2 are shown on a right hand side. Furthermore, a message exchange between the mobile devices MD1, MD2 via the D2D communication channel DDC is show schematically over time by means of arrows which indicate a source and destination of the message. Moreover, rounded rectangles are used to indicate steps being performed by either of the mobile devices MD1, MD2, with a horizontal position of a rectangle indicating on which subsystem the step is performed.

A match of the virtual network identity may be determined as follows. Firstly, the first mobile device MD1 sends a message to the second mobile device MD2 over the D2D communication channel, the message comprising many or all of the virtual network identities which are stored on the first mobile device MD1. In response, in a step titled DET_OVERLAP_STEP, the second mobile device MD2 determines which of the virtual network identities of the first mobile device MD1 overlap with those stored locally, i.e., on the second mobile device MD2. Moreover, in a step titled ORDER_STEP, the overlapping virtual network identities are ordered according to a priority list of the second mobile device MD2, and a result thereof is sent by message to the first mobile device MD1. Upon receipt, in a step titled SELECT_STEP, the overlapping virtual network identities are also ordered according to a priority list of the first mobile device MD1, and one of the overlapping virtual network identities is selected which ranks highest when combining both priority lists. Finally, the selected virtual network identity is sent by message to the second mobile device MD2, which in turn acknowledges the selected virtual network identity by return message.

The verifying the validity of the initiation key may comprise the aforementioned determining of the match of the virtual network identity on each of the mobile devices via the D2D communication channel. Consequently, if no matching virtual network identity can be found, the initiation keys on both mobile devices may be considered invalid for the purpose of establishing a D2D communication session between the mobile devices MD since said keys are associated with non-matching virtual network identities.

Having verified the match of the virtual network identity, the establishing of the D2D communication session may continue as follows. Each of the mobile devices MD1, MD2 may be arranged for performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key. Fig. 5 shows an example 162 of such a key synchronization procedure. This particular example is based on an exchange of one or more of the set of key identifiers between the mobile devices MD1, MD2. Here, upon request from the mobile subsystem MS1, the computing subsystem CS1 searches for a key identifier which is associated with a valid initiation key, meaning that said initiation key is valid at the current time and has not been used before in establishing a D2D communication session. The computing subsystem CS1 may search for the key identifier based on various criteria, such as, e.g., whether a key identifier is valid at the current time and a reasonable period in the future, e.g., the next 15 minutes. The search may also be based on a key sequence number associated with each of the key identifiers, with the computing

subsystem CS1 selecting one of the key identifiers that is associated with a lowest key sequence number. In case the key identifiers are numerical, the computing subsystem CS1 may also select a lowest one of the key identifiers. In case the key identifiers are sequentially ordered, the computing subsystem CS1 may also select a first or last one of the key identifiers. It will be appreciated that various criteria such as the above may be combined.

The computing subsystem CS1 sends the key identifier KeyID which was found to the mobile subsystem MS1, which in turn sends it to the second mobile device MD2. On the second mobile device MD2, the mobile subsystem MS2 forwards the key identifier KeyID to the computing subsystem CS2. Moreover, the second mobile device MD2 also performs a same process, either in parallel or after receiving the key identifier KeyID from the first mobile device MD1. As a result, the computing subsystems CS1, CS2 on each mobile device MD1, MD2 comprise both key identifiers. Each computing subsystem CS1, CS2 then selects, in a step titled MAX_KEYID_STEP, the key identifier which is highest, thereby also selecting the initiation key which is identified by said key identifier.

It is noted that, in general, initiation keys may be disabled or removed after use in establishing a D2D communication session. In this case, however, certain types of key synchronization procedures, such as the example shown in Fig. 5, may lead to a rapid consumption of initiation keys. Alternatively, the first mobile device MD1 may send the key identifier to the second mobile device MD2. The second mobile device MD2 may request its computing subsystem CS2 to determine if it comprises a valid initiation key associated with this key identifier. If so, the initiation key may be directly selected. If not, the computing subsystem CS2 may search for a lowest key identifier which is associated with a valid initiation key, and return the found key identifier to the mobile subsystem MS2 for sending to the first mobile device MD1. Upon receipt, the first mobile device MD1 may request its computing subsystem CS1 to determine if it comprises a valid initiation key associated with this key identifier. If so, the initiation key may be directly selected. If not, the computing subsystem CS1 may search for a lowest key identifier and again repeat the above process.

It is noted that the above alternative key synchronization procedure may be repeated several times. Alternatively, the key synchronization procedure may be based on an exchange of many or all key identifiers available to each respective mobile device so as to more rapidly determine a key identifier that identifies a matching and valid initiation key.

It is further noted that the key exchange procedure may be combined with an authentication procedure. The authentication procedure may be a prerequisite part of the setup of the D2D communication session. As a result, messages which are exchanged

between the mobile devices may serve both for the purpose of authentication as well as for key exchange. Figs. 7 and 8 show an example of this. For example, a message may constitute a challenge response from one mobile device while at the same time being part of the key exchange procedure between the mobile devices.

Having selected a matching one of the set of initiation keys on each of the mobile devices as the initiation key, the establishing of the D2D communication session may continue by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel. Fig. 6 shows an example 164 of a first part of such a key agreement procedure, which comprises using the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret. This first part of the key agreement procedure may be used to initialize a key exchange procedure based on the shared secret. Essentially, the first part of the key agreement procedure may be considered as a bootstrapping of the subsequent key exchange. An example of such a key exchange procedure is the Diffie-Hellman key exchange as known from the field of cryptography.

In the example of Fig. 6, each of the computing subsystems CS1, CS2 retrieves the initiation key from the storage area. In a step titled ENC_SECRET1_STEP, the computing subsystem CS1 of the first mobile device MD1 creates a message which comprises a secret, i.e., secret1, encrypted with the initiation key. The message is forwarded to the mobile subsystem MS1 which in turn sends the message to the second mobile device MD2. Here, the mobile subsystem MS2 forwards the message to the computing subsystem CS2. In a step titled DEC_SECRET1_STEP, the computing subsystem CS2 decrypts the message with the initiation key. In a step titled ENC_SECRET2_STEP, the computing subsystem CS2 creates a message with another secret, i.e., secret 2, encrypted with the initiation key. Moreover, in a step titled CALC_SK_STEP, a session key SK is calculated based on the combination of both secrets, i.e., secret1 and secret2, and included in the message. The message is sent back by the second mobile device MD2 to the first mobile device MD1. Here, the mobile subsystem MS1 forwards the message to the computing subsystem CS1. In a step titled DEC_SECRET2_STEP, the computing subsystem CS1 decrypts the message with the initiation key. In a step titled CALC_SK_STEP, the session key SK is calculated based on the combination of both secrets. As a result, on each of the computing subsystems CS1, CS2, both secrets are available, i.e., secret1 and secret2, thus allowing the respective computing subsystems to calculate a same session key SK.

It is noted that instead of the example of Fig. 6, various alternative mechanisms may be used as well for obtaining the shared secret. For example, one of the

point-to-point key establishment mechanisms as described in the ISO/IEC 11770-2 standard may be used. For example, the key establishment mechanism 5 as described in section 6.5 of said document may be used.

As a result of the subsequent key exchange procedure, a session key is obtained on each of the mobile devices MD1, MD2. This allows the D2D communication session to be established over the D2D communication channel based on the session key.

A second detailed embodiment comprises preloading a so-termed master key on each of the mobile devices MD1, MD2. Here, the term master key refers to an initiation key which is combined with a usage count so as to allow multiple D2D communication sessions to be established using one initiation key. The initiation key and the usage count constitute an alternative to the preloading of a plurality of initiation keys which may each be used only once in establishing a D2D communication session. It is noted that the initiation key may constitute a master key in that, each time an initiation key is needed for establishing a particular D2D communication session, a temporary initiation key is derived from the master key for that purpose. Hence, the initiation key may be used multiple times to establish a temporary initiation key for use in a particular D2D communication session. The mobile network MN may provide the computing subsystem CS1, CS2 of each mobile device MD1, MD2 with such an initiation key, the initiation key being valid for a particular validity period. Moreover, the mobile network MN may provide or set the usage count. The usage count may represent, e.g., a number of time the computing subsystem is allowed to generate a session key using the initiation key. The mobile network MN may also periodically provide the current network time so as to enable each computing subsystem CS1, CS2 to dispose of any initiation keys stored in the computing subsystem which have already expired according to the current network time. Additionally or alternatively, the mobile network MN may provide the current network time when preloading an initiation key on a mobile device MD1, MD2.

After having possibly verified a match of a virtual network identity, the validity of the initiation key is verified based on a current time and the usage count, and if the initiation key is deemed valid, the initiation key is used in performing a key agreement procedure between the mobile devices over the D2D communication channel. An example 166 of this is shown in Fig. 7, where the key agreement procedure is shown which is based on a three-pass authentication procedure, as specified by, e.g., the ISO/IEC 9798-4 standard.

Initially, each computing subsystems CS1, CS2 provides an identifier, i.e., ID1 and ID2, respectively, to each respective mobile subsystem MS1, MS2. Each identifier ID1, ID2, identifies the respective mobile device MD1, MD2. The identification may be

indirect in that each identifier ID1, ID2 may identify the respective computing subsystem CS1, CS2, which in turn allows the mobile device MD1, MD2 to be identified since the computing subsystem CS1, CS2 is an integral or removable part of the mobile device.

The further steps shown in Fig. 7 may be explained as follows. Here, the numerals correspond to those shown in Fig. 7.

1. The first mobile device MD1, being in this example the mobile device initiating the key agreement procedure, requests the computing subsystem CS1 to provide an key identifier KeyID which identifies an initiation key that is valid at the current time. The computing subsystem CS1 determines, in a step titled SELECT_KEYID_STEP, whether it comprises such an initiation key and if so, whether usage of the initiation key is still allowed, e.g., by checking whether the usage count is still below a given threshold in case the usage count corresponds to a number of uses, or whether the usage count is still above zero in case the usage count corresponds to a number of remaining uses. If this is the case, the initiation key is considered to be valid, and the computing subsystem CS1 establishes a key identifier KeyID identifying the initiation key. Moreover, the computing subsystem CS1 generates a random RND1, the random RND1 constituting a challenge in the authentication of the computing subsystem CS2 of the second mobile device MD2.

2. The computing subsystem CS1 provides the key identifier KeyID and the random RND1 to the mobile subsystem MS1 of the first mobile device MD1.

3. The first mobile device MD1 sends the key identifier KeyID, the random RND1 and the identifier ID1 to the second mobile device MD2 over the D2D communication channel DDC so as to initialize the key agreement procedure.

4. In response, the second mobile device MD2 requests its computing subsystem CS2 to initiate the key agreement procedure. For that purpose, it provides the key identifier KeyID, the random RND1 and the identifier ID1 to the computing subsystem CS2. In addition, the computing subsystem CS2 may request the second mobile device MD2 to provide the current time so as to enable the computing subsystem CS2 to verify if the initiation key identified by the key identifier KeyID is valid for the current time. This constitutes an additional verification step on the receiving, i.e., non-initializing, end of the key agreement procedure. When the initiation key identified by the key identifier KeyID is available to the computing subsystem CS2 and if usage of the initiation key is still allowed, e.g., in case its usage count is still above zero, the computing subsystem CS2 generates, in a step titled CALC_RESP1_STEP, a random RND2 and a session key SK_A for the authentication. The computing subsystem CS2 further calculates a response to the challenge

from the first mobile device MD1, being indicated as $E\_SK_A(X)$ with X = RND1 || RND2 || ID2. Here, the E_SK_A denotes an encryption function that uses SK_A as the session key and X as the message. An example of such a function is a Message Authentication Code (MAC).

5. The computing subsystem CS2 provides $E\_SK_A(X)$ and the random RND2 to the mobile subsystem MS2 of the second mobile device MD2.

6. The second mobile device MD2 sends $E\_SK_A(X)$, the random RND2 and the identifier ID2 to the first mobile device MD1, constituting a response to step 3.

7. The first mobile device MD1 requests its computing subsystem CS1 to authenticate the response received from the second mobile device MD2 and to generate a response to the challenge provided in the form of RND2.

8. In a step titled CALC_RESP2_STEP, the computing subsystem CS1 generates a session key for authentication of SK_A, and checks the response $E\_SK_A(X)$ from the second mobile device MD2. The computing subsystem CS1 then calculates a response to the challenge from the second mobile device MD2, being indicated by $E\_SK_A(Y)$ with Y = RND2 || RND1 || ID1. The computing subsystem CS1 generate a session key for use in the D2D communication session SK_C, and optionally a session key for integrity protection SK_I. The computing subsystem CS1 may then adjust, e.g., decrease, the usage count of the initiation key. Finally, the computing subsystem CS1 provides $E\_SK_A(Y)$, the session key SK_C, and optionally SK_I, to the mobile subsystem MS1.

9. The first mobile device MD1 sends a response to the challenge from the second mobile device MD2 in the form of $E\_SK_A(Y)$ to the second mobile device MD2.

10. In response, the second mobile device MD2 requests its computing subsystem CS2 to check, i.e., authenticate, $E\_SK_A(Y)$.

11. The computing subsystem CS2 then determines, in a step titled CALC_SESSIONKEY_STEP, if $E\_SK_A(Y)$ is valid, and if so generates the session key SK_C, and optionally SK_I, and provides both to the mobile subsystem MS2. The computing subsystem CS2 may then adjust, e.g., decrease, the usage count of the initiation key.

12. The mobile subsystem MS2 of the second mobile device MD2 establishes the D2D communication session with the mobile subsystem MS1 of the first mobile device MD1 using the session key SK_C. Hence, a secure D2D communication session is obtained.

Fig. 8 shows an alternative 168 to the key agreement procedure 166 as shown in Fig. 7. A difference concerns that here, the identifiers ID1 and ID2 are encrypted during exchange, whereas in the key agreement procedure of Fig. 7, the identifiers ID1 and ID2 were exchanged without being encrypted. By encrypting the identifiers ID1 and ID2 during

exchange, it may be prevented that users are tracked and/or identified through eavesdropping of the message exchange between the mobile devices MD1, MD2.

The further steps shown in Fig. 8 may be explained as follows. Here, the numerals correspond to those shown in Fig. 8.

1. Step 1 corresponds to step 1 as discussed in reference to Fig. 7, with the addition that the computing subsystem CS1 generates a challenge, being essentially a message that is encrypted using the initiation key, the encrypted message being denoted by E_MK, and the encrypted message comprising the random RND1 and the identifier ID1.

2. The computing subsystem CS1 provides the key identifier KeyID and the challenge to the mobile subsystem MS1 of the first mobile device MD1.

3. The first mobile device MD1 sends the key identifier KeyID, the challenge to the second mobile device MD2 over the D2D communication channel DDC so as to initialize the key agreement procedure.

4. In response, the second mobile device MD2 requests its computing subsystem CS2 to initiate the key agreement procedure. For that purpose, it provides the key identifier KeyID, the challenge to the computing subsystem CS2. In addition, the computing subsystem CS2 may request the second mobile device MD2 to provide the current time so as to enable the computing subsystem CS2 to verify if the initiation key identified by the key identifier KeyID is valid for the current time. This constitutes an additional verification step on the receiving, i.e., non-initializing, end of the key agreement procedure. When the initiation key identified by the key identifier KeyID is available to the computing subsystem CS2 and if usage of the initiation key is still allowed, e.g., in case its usage count is still above zero, the computing subsystem CS2 generates, in a step titled CALC_RESP1_STEP, a random RND2 and a session key SKA for the authentication. The computing subsystem CS2 further calculates a response to the challenge from the first mobile device MD1, being indicated as E_SKA(X) with X = RND1 || RND2 || ID2. Here, the E_SKA denotes an encryption function that uses SKA as the session key and X as the message. An example of such a function is a Message Authentication Code (MAC). The computing subsystem CS2 also calculates a challenge, E_MK(RND2||ID2), for which the same E_MK is used that the computing subsystem CS1 of the first mobile device MD1 used in its challenge.

5. The computing subsystem CS2 provides E_SKA(X) and the challenge to the mobile subsystem MS2 of the second mobile device MD2.

6. The second mobile device MD2 sends E_SKA(X) and the challenge to the first mobile device MD1, constituting a response to step 3.

7. The first mobile device MD1 requests its computing subsystem CS1 to authenticate the response received from the second mobile device MD2 and to generate a response to the challenge provided in the form of E_MK(RND2||ID2).

8-12. Steps 8-12 correspond to steps 8-12 as discussed in reference to Fig. 7.

It is noted that in general, a computing subsystem of a mobile device may request a further initiation key via the mobile network if i) no initiation key is deemed valid, or ii) the key agreement procedure fails in providing the session key.

It will be appreciated that the present invention may be advantageously applied to Direct LTE, i.e., LTE-based D2D communication between mobile devices. In particular, the present invention allows the following advantageous uses.

Corporation X has purchased a direct mode subscription from operator Y for all its employees. As a result, for example once a week during the night or during low network load, all mobile devices of the corporation, such as mobile phones and dongles, are provided with a set of a hundred initiation keys which are valid for every day of the following week. On a next Monday, several employees have a meeting in which they would like to share a presentation. However, they are located in a meeting room without network coverage, i.e., are outside a range of the mobile network. They plug-in their dongles into their laptops and setup an ad hoc network based on Direct LTE. Since all dongles were provided with a same set of initiation keys, the employees are able to setup a LTE-based D2D communication session in the meeting room without needing to access the mobile network.

Another advantageous use may be the following. Again, corporation X has purchased a direct mode subscription. Again, for example once a week during the night or during low network load, all mobile devices of the corporation are provided with a set of a hundred initiation keys which are valid for every day of the following week. However, one dongle was turned off during said preloading procedure. On a next Monday, several employees have a meeting in which they would like to share a presentation. They are located in a room with network coverage. They plug-in their dongles into their laptops and setup an ad hoc network based on Direct LTE. Because most of the dongles were provided with a same set of initiation keys, the employees are able to setup a LTE-based D2D communication session in the meeting room without needing to access the mobile network. However, the dongle which was turned off during the preloading procedure can still join the D2D communication session by requesting from the mobile network the set of initiation keys, and once said set has been provided, the dongle joins the D2D communication session.

Another advantageous use may be the following, which is a same as the aforementioned use, except that the employees are located in a room with network coverage. They plug-in their dongles into their laptops and setup an ad hoc network based on Direct LTE. Some dongles already have keys available for the D2D communication session, but some only have expired keys, e.g., because D2D communication hasn't been used for some time and therefore no initiation keys needed to be preloaded or updated. All dongles now request from the mobile network a set of initiation keys and once said set has been provided, each dongle joins the D2D communication session. Later that day, the employees meet again. Now, a D2D communication session can be established immediately, i.e., without a need to contact the mobile network, since the dongles now already have a set of valid initiation keys.

Yet another advantageous use may the following. For emergency services, it is of utmost importance to be able to communicate at all times. Hence, a mobile device which relies on network coverage to establish a D2D communication session may not be desirable. This may be avoided by preloading initiation keys frequently, e.g., every time when a mobile device is switched on, and/or by preloading initiation keys which are associated with a validity period that is relatively long. The preloading may also occur every night, when all the mobile devices are at a central location. During the day, the firefighters, policemen and ambulance personnel can choose direct mode operation in case network reception is inadequate, thereby still allowing communication amongst said emergency service personnel.

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative embodiments.

In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. Use of the verb "comprise" and its conjugations does not exclude the presence of elements or steps other than those stated in a claim. The article "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. The invention may be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In the device claim enumerating several means, several of these means may be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

CLAIMS

1. Method (100) for establishing a device-to-device [D2D] communication session between mobile devices (MD1, MD2) which are mutually connectable via a D2D communication channel (DDC) and individually connectable to a mobile network (MN), comprising:

- preloading (120) an initiation key on each of the mobile devices (MD1, MD2), the initiation key being associated with a validity period; and

on each of the mobile devices (MD1, MD2):

- verifying (140) a validity of the initiation key based on a current time;
- if the initiation key is deemed valid, generating (160) a session key using the initiation key by using the initiation key in performing (164, 166) a key agreement procedure between the mobile devices (MD1, MD2) over the D2D communication channel (DDC), the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and
- establishing (180) the D2D communication session over the D2D communication channel (DDC) based on the session key.

2. Method (100) according to claim 1, wherein the preloading (120) the initiation key comprises providing the initiation key to each of the mobile devices (MD1, MD2) via the mobile network (MN) when each respective mobile device is connected to the mobile network.

3. Method (100) according to claim 1 or 2, wherein the preloading (120) the initiation key comprises storing the initiation key in a secure storage area (SA1) of each respective mobile device (MD1, MD2).

4. Method (100) according to claim 3, wherein the secure storage area (SA1) is provided by a trusted computing subsystem (CS1, CS2) of each respective mobile device (MD1, MD2).

5. Method (100) according to claim 4, wherein at least one of the group of: verifying (140) the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem (CS1, CS2).

6. Method (100) according to any one of the above claims, further comprising:

- preloading (120) a set of initiation keys on each of the mobile devices (MD1, MD2), the set of initiation keys key being associated with a respective set of validity periods; and

- performing (162) a key synchronization procedure between the mobile devices (MD1, MD2) over the D2D communication channel (DDC) for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.

7. Method (100) according to claim 6, further comprising:

- preloading (120) a set of key identifiers on each of the mobile devices (MD1, MD2), each of the set of key identifiers identifying a respective one of the set of initiation keys; and

- performing (162) the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.

8. Method (100) according to claim 6 or 7, further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session.

9. Method (100) according to any one of claims 6-8, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods.

10. Method (100) according to any one of the above claims, wherein the initiation key is associated with a virtual network identity, and wherein the verifying (140) the validity of the initiation key further comprises determining (142) a match of the virtual network identity on each of the mobile devices (MD1, MD2) via the D2D communication channel (DDC).

11. Method (100) according to any one of the above claims, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and

wherein the verifying (140) the validity of the initiation key is further based on the usage count.

12. Method (100) according to claim 11, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session.

13. Method (100) according to any one of the above claims, further comprising requesting a further initiation key via the mobile network (MN) if i) no initiation key is deemed valid, or ii) the key agreement procedure fails in providing the session key.

14. Method according to any one of the above claims, wherein the key agreement procedure comprises:

- a three-pass authentication procedure (166); or
- a use (164) of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.

15. Control software comprising instructions for, upon execution of the control software on a mobile device (MD1, MD2), causing the mobile device to establish the D2D communication session according to the method of any one of the above claims.

16. Mobile device (MD1) for establishing a device-to-device [D2D] communication session with a further mobile device (MD2), the mobile device and the further mobile device being mutually connectable via a D2D communication channel (DDC) and individually connectable to a mobile network (MN), the mobile device comprising:

- a storage area (SA1) for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and
- a computing subsystem (CS1) for:
  - verifying a validity of the initiation key based on a current time;
  - if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device (MD2) over the D2D communication channel (DDC), the key agreement procedure resulting in the session key if the initiation key used by the mobile device and the further mobile device matches; and

- a mobile subsystem (MS1) for establishing the D2D communication session over the D2D communication channel based on the session key.

17. Mobile network (MN) arranged for preloading an initiation key on a mobile device (MD1) according to claim 16 when the mobile device is connected to the mobile network, the initiation key being associated with a validity period.

ABSTRACT

Method (100) for establishing a device-to-device [D2D] communication session between mobile devices (MD1, MD2) which are mutually connectable via a D2D communication channel (DDC) and individually connectable to a mobile network (MN), comprising:

- preloading (120) an initiation key on each of the mobile devices (MD1, MD2), the initiation key being associated with a validity period; and

on each of the mobile devices (MD1, MD2):

- verifying (140) a validity of the initiation key based on a current time;
- if the initiation key is deemed valid, generating (160) a session key using the initiation key by using the initiation key in performing (164, 166) a key agreement procedure between the mobile devices (MD1, MD2) over the D2D communication channel (DDC), the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and
- establishing (180) the D2D communication session over the D2D communication channel (DDC) based on the session key.

Figure 1

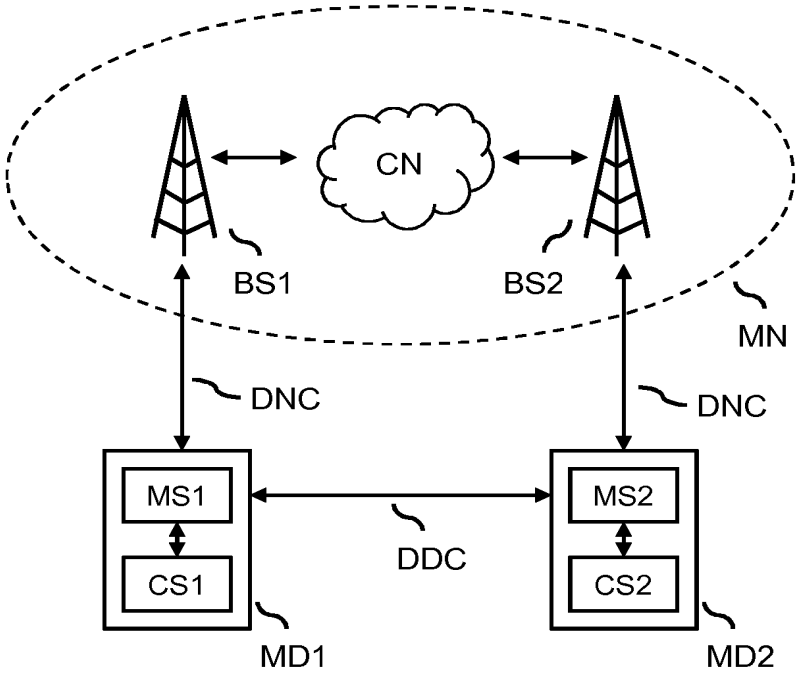


Fig. 1

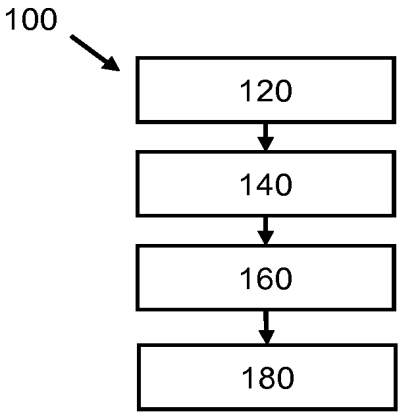


Fig. 2

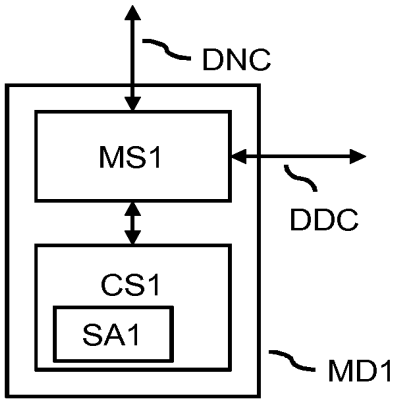


Fig. 3

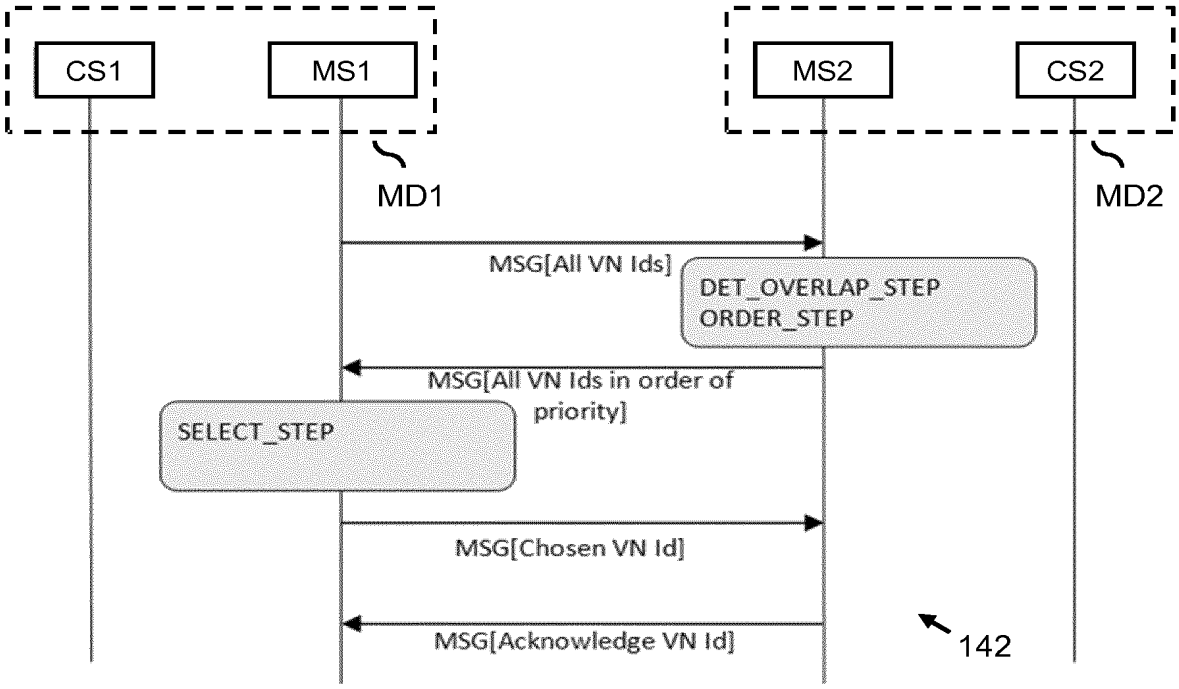

CS1
MS1
MS2
CS2
MD1
MD2
MSG[All VN Ids]
DET_OVERLAP_STEP
ORDER_STEP
MSG[All VN Ids in order of priority]
SELECT_STEP
MSG[Chosen VN Id]
MSG[Acknowledge VN Id]
142

Fig. 4

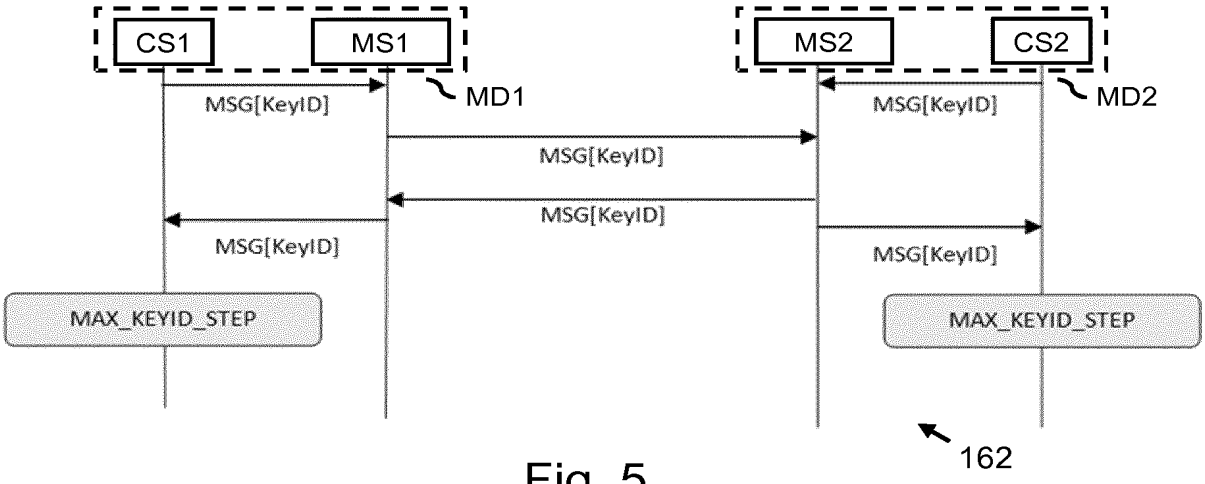

CS1
MS1
MS2
CS2
MD1
MD2
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MAX_KEYID_STEP
MAX_KEYID_STEP
162

Fig. 5

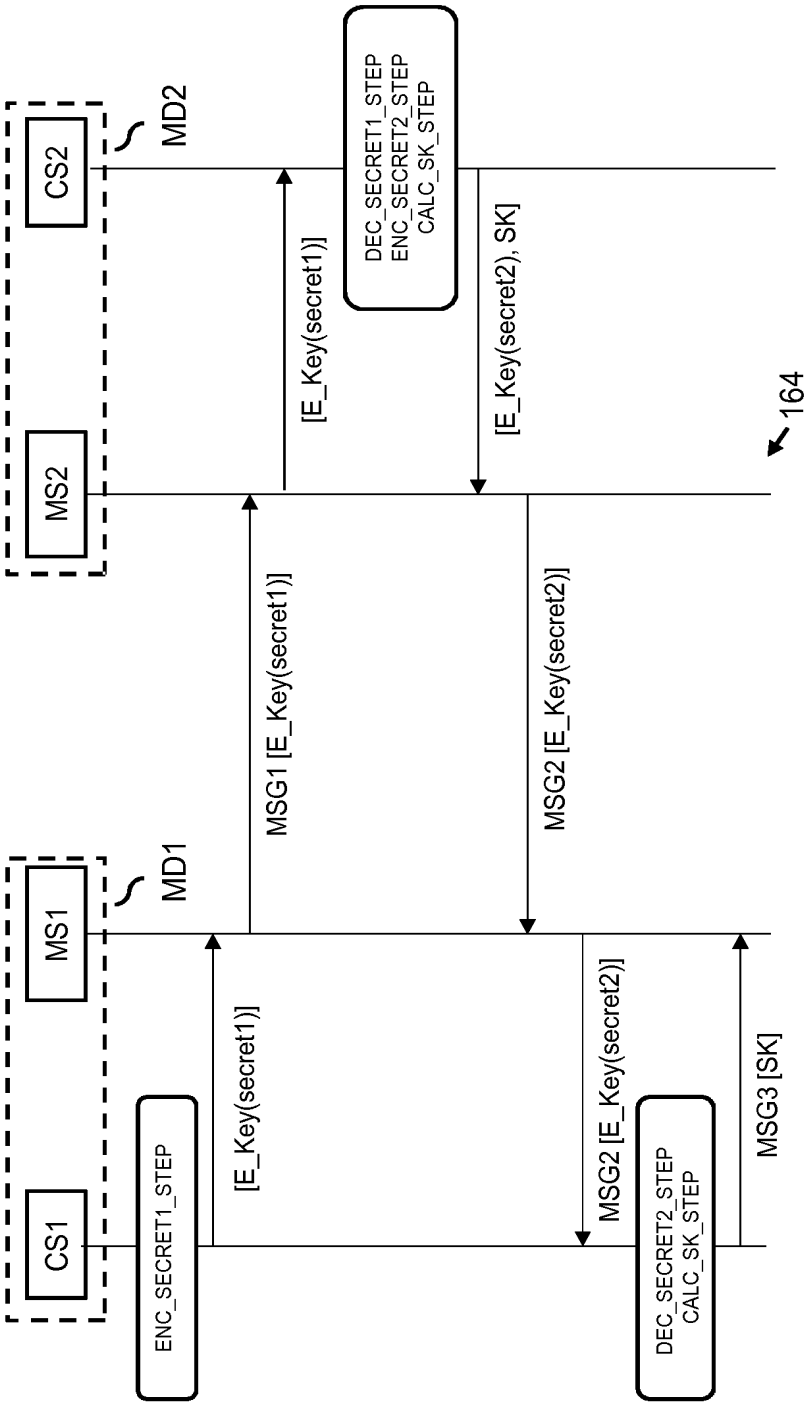

CS1
MS1
MD1
CS2
MS2
MD2
ENC_SECRET1_STEP
[E_Key(secret1)]
MSG1 [E_Key(secret1)]
DEC_SECRET1_STEP
ENC_SECRET2_STEP
CALC_SK_STEP
[E_Key(secret2), SK]
MSG2 [E_Key(secret2)]
MSG2 [E_Key(secret2)]
DEC_SECRET2_STEP
CALC_SK_STEP
MSG3 [SK]
164

Fig. 6

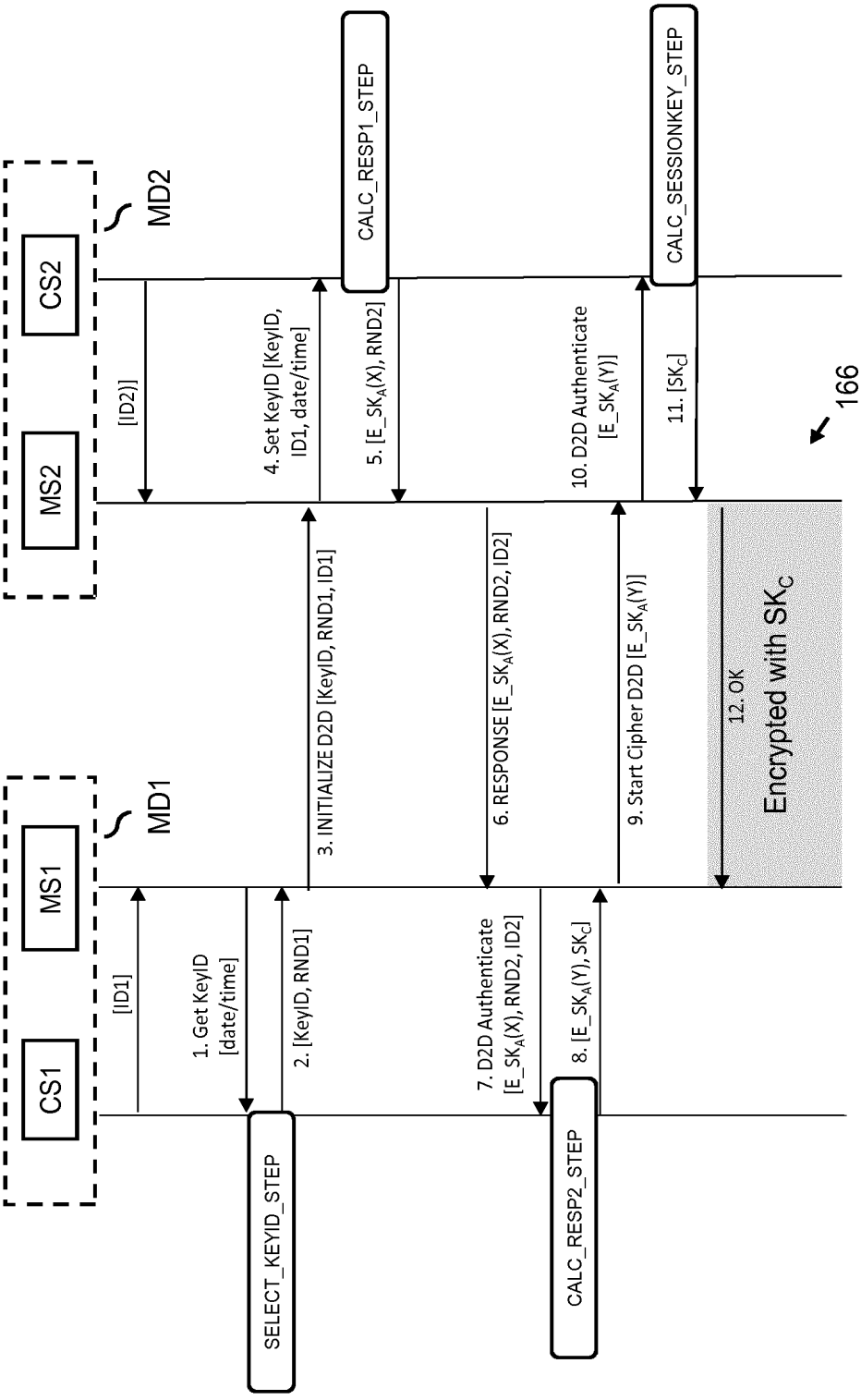

CS1
MS1
MD1
CS2
MS2
MD2
[ID1]
1. Get KeyID [date/time]
2. [KeyID, RND1]
3. INITIALIZE D2D [KeyID, RND1, ID1]
[ID2)]
4. Set KeyID [KeyID, ID1, date/time]
5. [E_SK$_A$(X), RND2]
6. RESPONSE [E_SK$_A$(X), RND2, ID2]
7. D2D Authenticate [E_SK$_A$(X), RND2, ID2]
8. [E_SK$_A$(Y), SK$_C$]
9. Start Cipher D2D [E_SK$_A$(Y)]
10. D2D Authenticate [E_SK$_A$(Y)]
11. [SK$_C$]
12. OK
Encrypted with SK$_C$
SELECT_KEYID_STEP
CALC_RESP2_STEP
CALC_RESP1_STEP
CALC_SESSIONKEY_STEP
166

Fig. 7

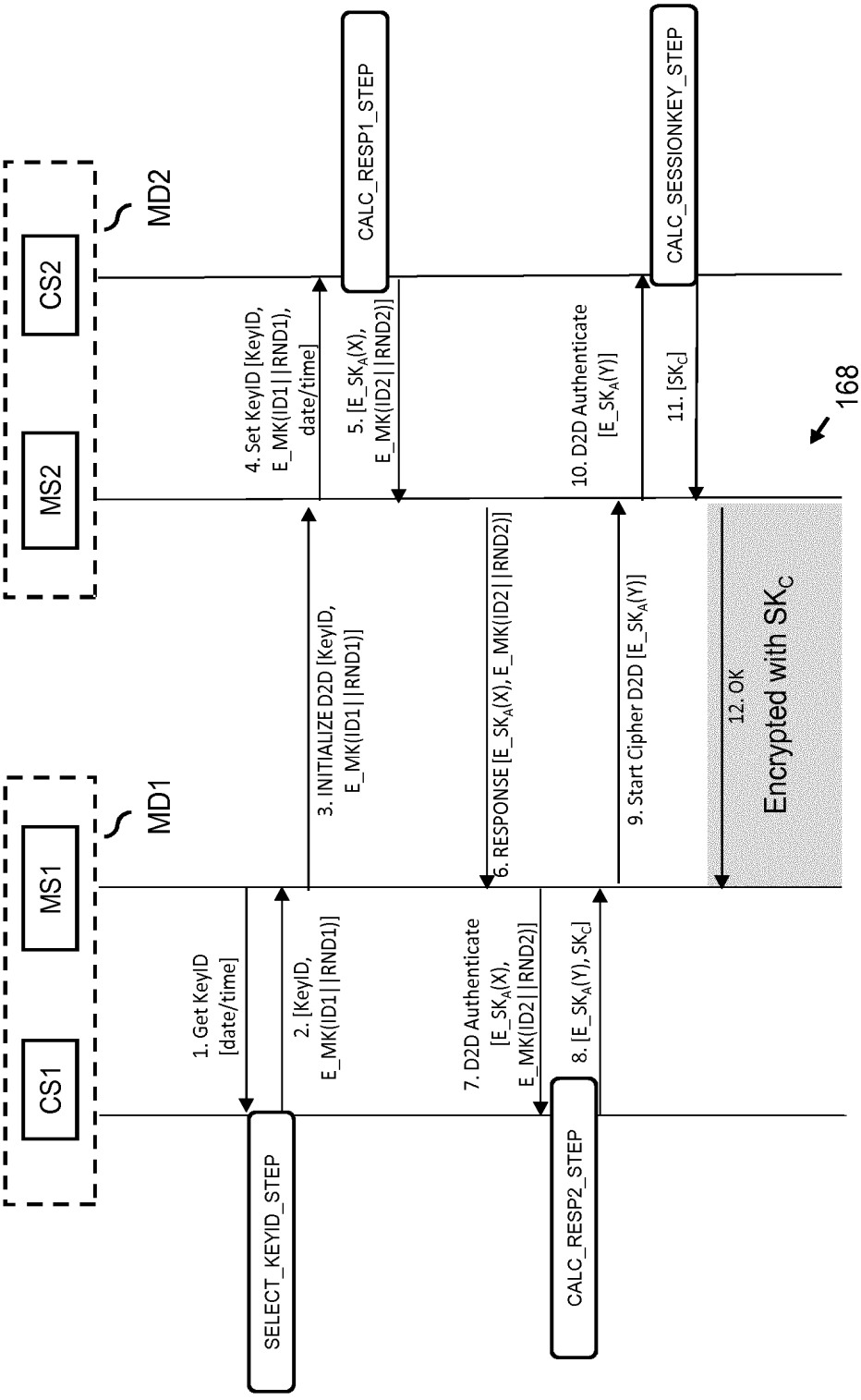

CS1
MS1
MD1
CS2
MS2
MD2
1. Get KeyID [date/time]
2. [KeyID, E_MK(ID1||RND1)]
3. INITIALIZE D2D [KeyID, E_MK(ID1||RND1)]
4. Set KeyID [KeyID, E_MK(ID1||RND1), date/time]
5. [E_SK_A(X), E_MK(ID2||RND2)]
6. RESPONSE [E_SK_A(X), E_MK(ID2||RND2)]
7. D2D Authenticate [E_SK_A(X), E_MK(ID2||RND2)]
8. [E_SK_A(Y), SK_C]
9. Start Cipher D2D [E_SK_A(Y)]
10. D2D Authenticate [E_SK_A(Y)]
11. [SK_C]
12. OK
Encrypted with SK_C
SELECT_KEYID_STEP
CALC_RESP2_STEP
CALC_RESP1_STEP
CALC_SESSIONKEY_STEP
168

Fig. 8

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/EP2013/067904**
International filing date:		**29 August 2013 (29.08.2013)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**EP**
	Number:	**12183256.2**
	Filing date:	**06 September 2012 (06.09.2012)**
Date of receipt at the International Bureau:		**19 September 2013 (19.09.2013)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

CLAIMS

1. Method (100) for establishing a device-to-device [D2D] communication session between mobile devices (MD1, MD2) which are mutually connectable via a D2D communication channel (DDC) and individually connectable to a mobile network (MN), comprising:

- preloading (120) an initiation key on each of the mobile devices (MD1, MD2), the initiation key being associated with a validity period; and

on each of the mobile devices (MD1, MD2):

- verifying (140) a validity of the initiation key based on a current time;
- if the initiation key is deemed valid, generating (160) a session key using the initiation key by using the initiation key in performing (164, 166) a key agreement procedure between the mobile devices (MD1, MD2) over the D2D communication channel (DDC), the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and
- establishing (180) the D2D communication session over the D2D communication channel (DDC) based on the session key.

2. Method (100) according to claim 1, wherein the preloading (120) the initiation key comprises providing the initiation key to each of the mobile devices (MD1, MD2) via the mobile network (MN) when each respective mobile device is connected to the mobile network.

3. Method (100) according to claim 1 or 2, wherein the preloading (120) the initiation key comprises storing the initiation key in a secure storage area (SA1) of each respective mobile device (MD1, MD2).

4. Method (100) according to claim 3, wherein the secure storage area (SA1) is provided by a trusted computing subsystem (CS1, CS2) of each respective mobile device (MD1, MD2).

5. Method (100) according to claim 4, wherein at least one of the group of: verifying (140) the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem (CS1, CS2).

6. Method (100) according to any one of the above claims, further comprising:

- preloading (120) a set of initiation keys on each of the mobile devices (MD1, MD2), the set of initiation keys key being associated with a respective set of validity periods; and
- performing (162) a key synchronization procedure between the mobile devices (MD1, MD2) over the D2D communication channel (DDC) for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.

7. Method (100) according to claim 6, further comprising:

- preloading (120) a set of key identifiers on each of the mobile devices (MD1, MD2), each of the set of key identifiers identifying a respective one of the set of initiation keys; and
- performing (162) the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.

8. Method (100) according to claim 6 or 7, further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session.

9. Method (100) according to any one of claims 6-8, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods.

10. Method (100) according to any one of the above claims, wherein the initiation key is associated with a virtual network identity, and wherein the verifying (140) the validity of the initiation key further comprises determining (142) a match of the virtual network identity on each of the mobile devices (MD1, MD2) via the D2D communication channel (DDC).

11. Method (100) according to any one of the above claims, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and

wherein the verifying (140) the validity of the initiation key is further based on the usage count.

12. Method (100) according to claim 11, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session.

13. Method (100) according to any one of the above claims, further comprising requesting a further initiation key via the mobile network (MN) if i) no initiation key is deemed valid, or ii) the key agreement procedure fails in providing the session key.

14. Method according to any one of the above claims, wherein the key agreement procedure comprises:

- a three-pass authentication procedure (166); or
- a use (164) of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.

15. Control software comprising instructions for, upon execution of the control software on a mobile device (MD1, MD2), causing the mobile device to establish the D2D communication session according to the method of any one of the above claims.

16. Mobile device (MD1) for establishing a device-to-device [D2D] communication session with a further mobile device (MD2), the mobile device and the further mobile device being mutually connectable via a D2D communication channel (DDC) and individually connectable to a mobile network (MN), the mobile device comprising:

- a storage area (SA1) for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and
- a computing subsystem (CS1) for:
  - verifying a validity of the initiation key based on a current time;
  - if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device (MD2) over the D2D communication channel (DDC), the key agreement procedure resulting in the session key if the initiation key used by the mobile device and the further mobile device matches; and

- a mobile subsystem (MS1) for establishing the D2D communication session over the D2D communication channel based on the session key.

17. Mobile network (MN) arranged for preloading an initiation key on a mobile device (MD1) according to claim 16 when the mobile device is connected to the mobile network, the initiation key being associated with a validity period.

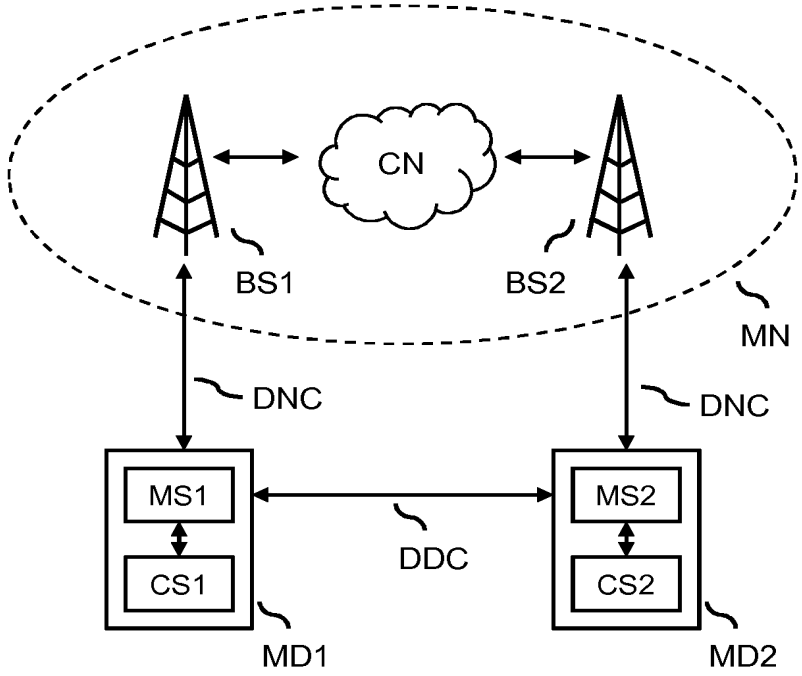


Fig. 1

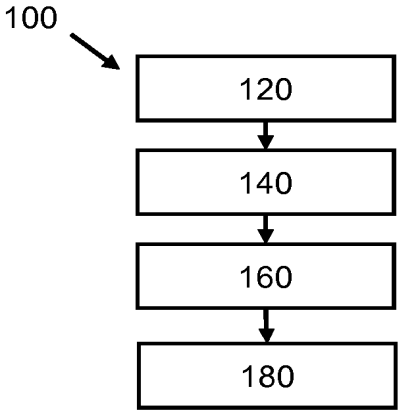


Fig. 2

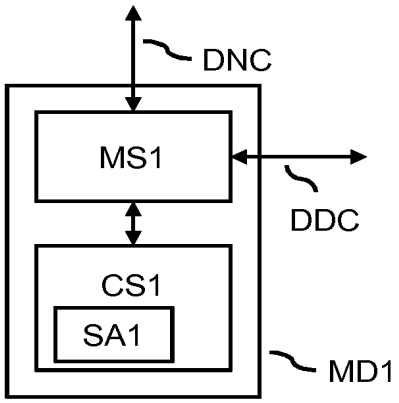


Fig. 3

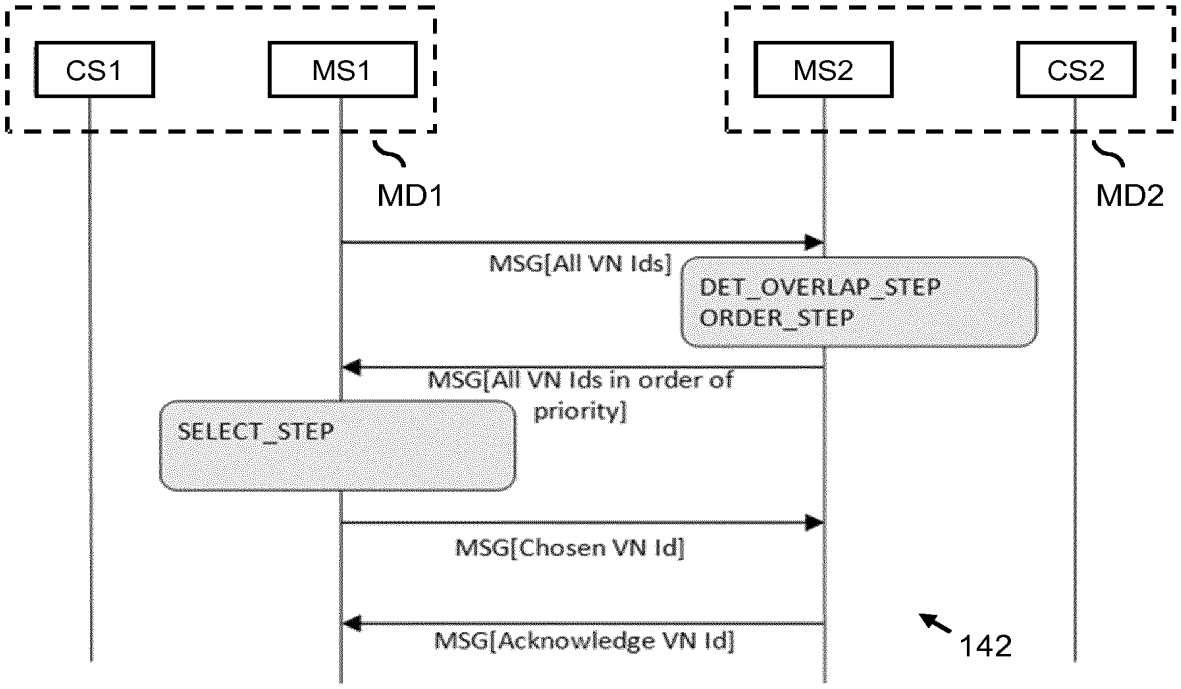

CS1
MS1
MS2
CS2
MD1
MD2
MSG[All VN Ids]
DET_OVERLAP_STEP
ORDER_STEP
MSG[All VN Ids in order of priority]
SELECT_STEP
MSG[Chosen VN Id]
MSG[Acknowledge VN Id]
142

Fig. 4

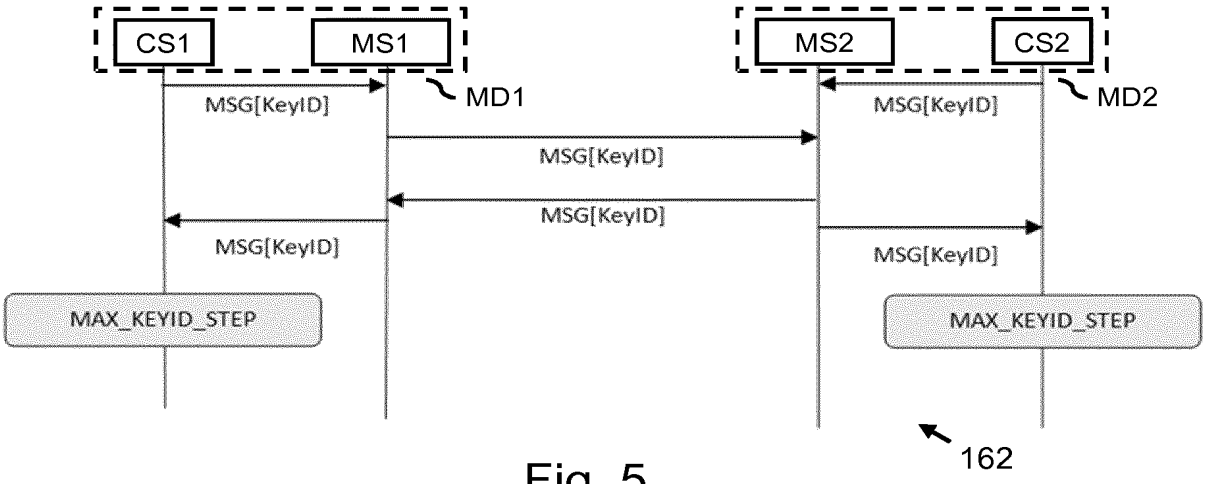

CS1
MS1
MS2
CS2
MD1
MD2
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MAX_KEYID_STEP
MAX_KEYID_STEP
162

Fig. 5

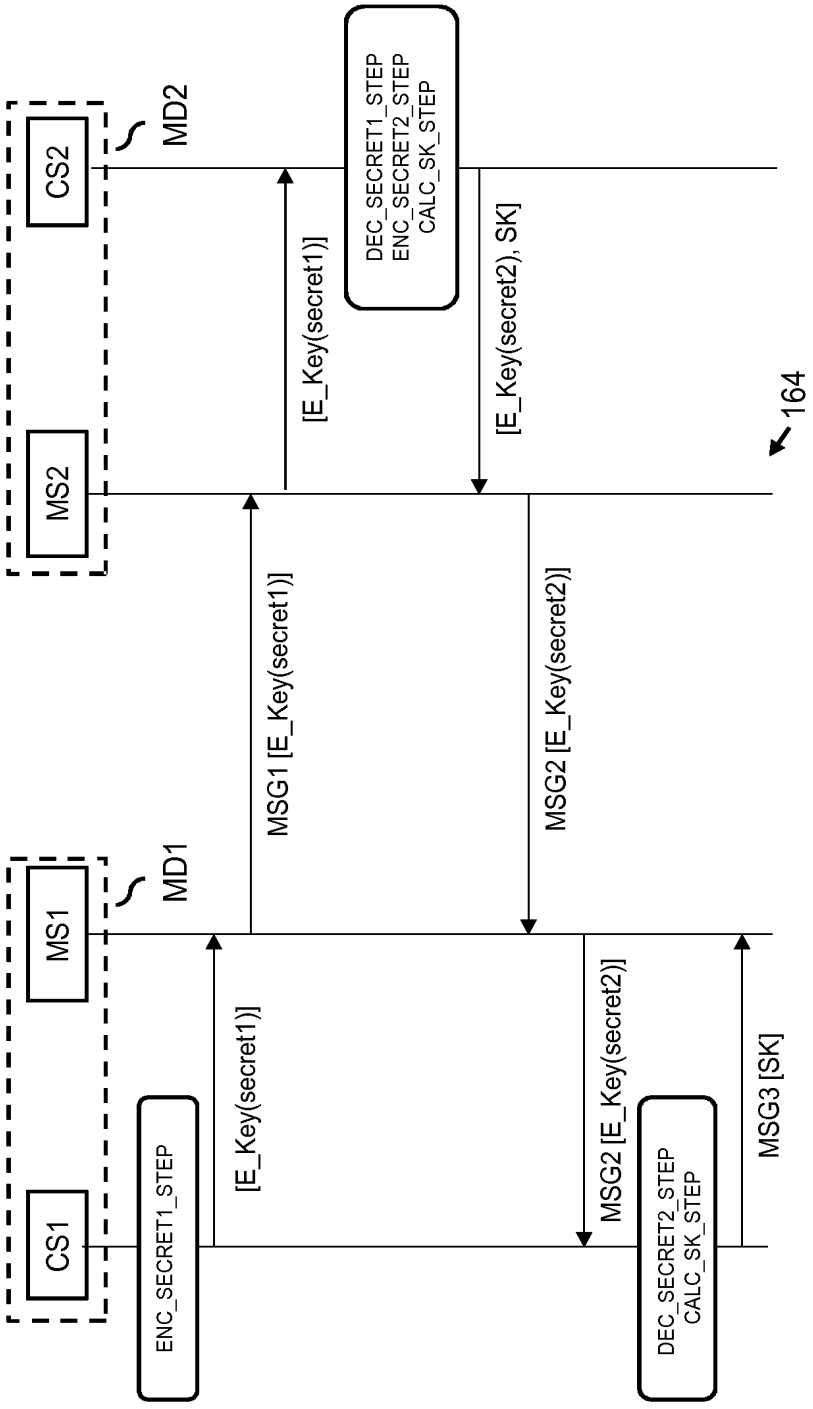

CS2
MD2
MS2
DEC_SECRET1_STEP
ENC_SECRET2_STEP
CALC_SK_STEP
[E_Key(secret1)]
[E_Key(secret2), SK]
164
MSG1 [E_Key(secret1)]
MSG2 [E_Key(secret2)]
MS1
MD1
CS1
ENC_SECRET1_STEP
[E_Key(secret1)]
MSG2 [E_Key(secret2)]
DEC_SECRET2_STEP
CALC_SK_STEP
MSG3 [SK]

Fig. 6

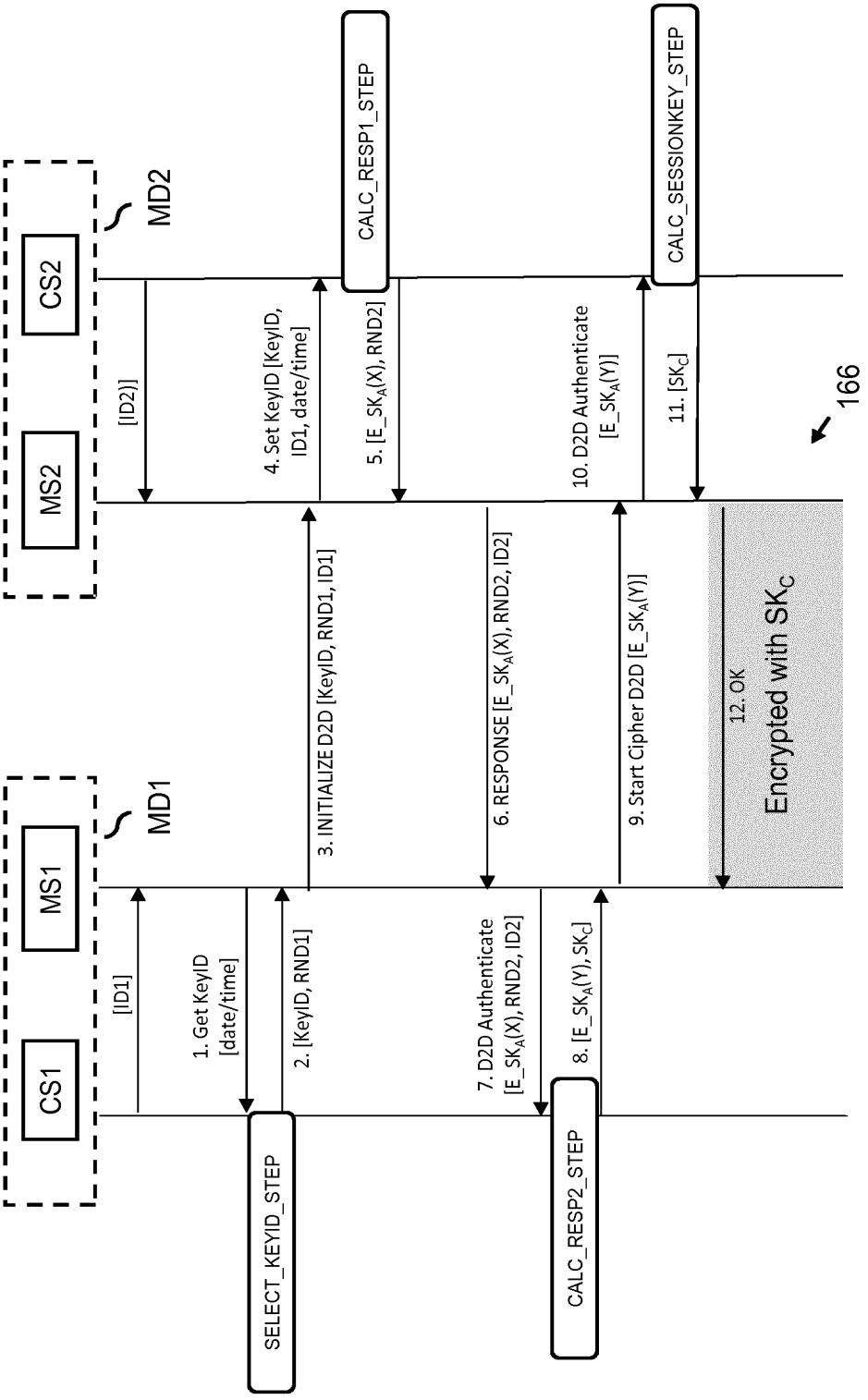

CS1
MS1
MD1
CS2
MS2
MD2
[ID1]
1. Get KeyID [date/time]
2. [KeyID, RND1]
3. INITIALIZE D2D [KeyID, RND1, ID1]
4. Set KeyID [KeyID, ID1, date/time]
[ID2]
5. [E_SK_A(X), RND2]
6. RESPONSE [E_SK_A(X), RND2, ID2]
7. D2D Authenticate [E_SK_A(X), RND2, ID2]
8. [E_SK_A(Y), SK_C]
9. Start Cipher D2D [E_SK_A(Y)]
10. D2D Authenticate [E_SK_A(Y)]
11. [SK_C]
12. OK
Encrypted with SK_C
SELECT_KEYID_STEP
CALC_RESP2_STEP
CALC_RESP1_STEP
CALC_SESSIONKEY_STEP
166

Fig. 7

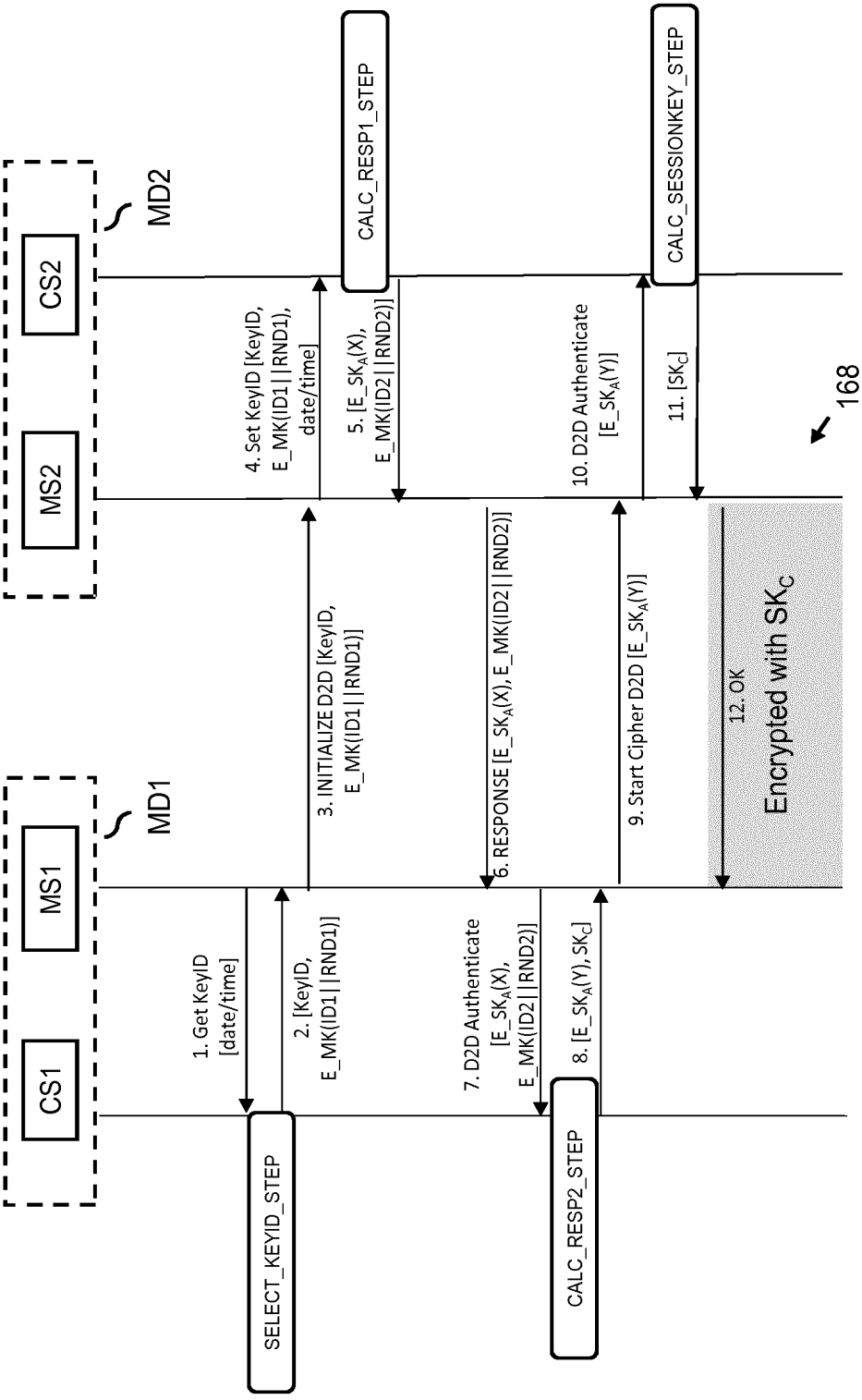

CS1
MS1
MD1
CS2
MS2
MD2
SELECT_KEYID_STEP
CALC_RESP2_STEP
CALC_RESP1_STEP
CALC_SESSIONKEY_STEP
1. Get KeyID [date/time]
2. [KeyID, E_MK(ID1||RND1)]
3. INITIALIZE D2D [KeyID, E_MK(ID1||RND1)]
4. Set KeyID [KeyID, E_MK(ID1||RND1), date/time]
5. [E_SK_A(X), E_MK(ID2||RND2)]
6. RESPONSE [E_SK_A(X), E_MK(ID2||RND2)]
7. D2D Authenticate [E_SK_A(X), E_MK(ID2||RND2)]
8. [E_SK_A(Y), SK_C]
9. Start Cipher D2D [E_SK_A(Y)]
10. D2D Authenticate [E_SK_A(Y)]
11. [SK_C]
12. OK
Encrypted with SK_C
168

Fig. 8

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 March 2014 (13.03.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/037277 A1

(51) **International Patent Classification**:
H04W 12/04 (2009.01) *H04W 76/02* (2009.01)
H04W 74/08 (2009.01)

(21) **International Application Number**:
PCT/EP2013/067904

(22) **International Filing Date**:
29 August 2013 (29.08.2013)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
12183256.2 6 September 2012 (06.09.2012) EP

(71) **Applicants**: **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**: **NORP, Antonius**; Cornelis Jolstraat 83, NL-2584 EN The Hague (NL). **FRANSEN, Frank**; Brilweg 21, NL-9801 GC Zuidhorn (NL). **DE KIEVIT, Sander**; Ravenhorst 61, NL-2317 AG Leiden (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, BN, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, 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**: ESTABLISHING A DEVICE-TO-DEVICE COMMUNICATION SESSION

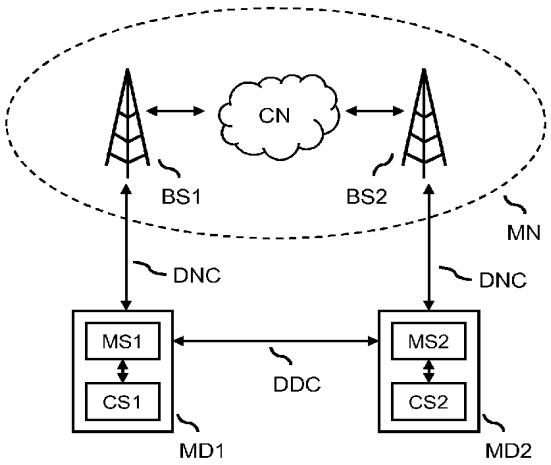


Fig. 1

(57) **Abstract**: A method is disclosed for establishing a device-to-device communication session between mobile devices (MD1, MD2) which are mutually connectable via a D2D communication channel (DDC) and individually connectable to a mobile network (MN), comprising: • - preloading (120) an initiation key on each of the mobile devices (MD1, MD2), the initiation key being associated with a validity period; and on each of the mobile devices (MD1, MD2): • - verifying (140) a validity of the initiation key based on a current time; • - if the initiation key is deemed valid, generating (160) a session key using the initiation key by using the initiation key in performing (164, 166) a key agreement procedure between the mobile devices (MD1, MD2) over the D2D communication channel (DDC), the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and • - establishing (180) the D2D communication session over the D2D communication channel (DDC) based on the session key.

WO 2014/037277 A1

Establishing a device-to-device communication session

FIELD OF THE INVENTION

The invention relates to a method for establishing a device-to-device (D2D) communication session between mobile devices. The invention further relates to a mobile device for establishing the D2D communication session with a further mobile device. The invention further relates to control software comprising instructions for execution on the mobile device. The invention further relates to the mobile network.

Mobile communication networks, also referred to as cellular networks or mobile networks, have been extensively deployed over the last decades in order to address the increasing need for mobile communication. Communication between mobile devices which are connected to such a mobile network typically takes place via the mobile network, i.e., via one or more base stations and core nodes of the mobile network.

BACKGROUND OF THE INVENTION

It is desirable to enable mobile devices which are typically connected to a mobile network to also directly communicate with each other, i.e., via so-termed device-to-device (D2D) communication.

D2D communication is characterized by a direct wireless communication path between two mobile terminals, such as the mobile devices, while maintaining, at least at some moments in time, at least a signaling connection with/via a base station of the wireless communication network, i.e., of the mobile network. The direct wireless communication path between mobile terminals allows to offload the base station(s), the access network and the core network of the wireless communication network from most of the data and signaling exchanged between the mobile terminals. The signaling connection with (a base station of) the wireless communication network allows the wireless communication network to control the resources assigned to the direct communication path between the terminals.

A mobile device which, at a given time, uses D2D communication instead of communicating via the mobile network may be referred to as operating in Direct Mode Operation (DMO). DMO offers advantages such as, e.g., enabling mobile communication

between users outside a range of the mobile network, reducing of load from the base stations and/or from the core nodes of the mobile network, etc.

An example of a mobile communication standard which enables mobile communication between mobile devices both via the mobile network as well as via the aforementioned D2D communication is Terrestrial Trunked Radio (TETRA).

Another example of such a mobile communication standard is Global System for Mobile Communications (GSM). The GSM standard includes a so-termed local call, local switch feature in which mobile communication between mobile devices which are connected to a same base station of the mobile network is not routed through the core nodes of the mobile network, but rather directly from the base station to each respective mobile device.

Yet another example is Long Term Evolution (LTE). Recent developments in LTE include D2D communication between mobile devices. It is noted that in the context of LTE, such D2D communication is also referred to as Direct LTE.

SUMMARY OF THE INVENTION

A problem of the above mobile networks and mobile devices is that an operator of the mobile network has no or only limited control over the D2D communication. The inventors have recognized that such control is desirable for various reasons. For example, the D2D communication may take place in a frequency spectrum which is licensed to the operator and thus needs to be managed by the operator, e.g., to avoid interference. Another example is that the operator may desire to only grant specific users access to the D2D communication, e.g., emergency workers, subscribers to a D2D service, etc.

It would be advantageous to provide more control over the D2D communication between mobile devices which are connectable to a mobile network.

To better address this concern, a first aspect of the invention provides a method for establishing a D2D communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:

- preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and

on each of the mobile devices:

- verifying a validity of the initiation key based on a current time;
- if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between

the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and

- establishing the D2D communication session over the D2D communication channel based on the session key.

A further aspect of the invention provides control software comprising instructions for, upon execution of the control software on a mobile device, causing the mobile device to establish the D2D communication session according to the method set forth.

A further aspect of the invention provides a mobile device for establishing a D2D communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:

- a storage area for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and
- a computing subsystem for:
  - verifying a validity of the initiation key based on a current time;
  - if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device and the further mobile device matches; and
  - a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

A further aspect of the invention provides a mobile network arranged for preloading an initiation key on the mobile device set forth when the mobile device is connected to the mobile network, the initiation key being associated with a validity period.

The aforementioned measures establish, or provide the means to establish a D2D communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network. Here, the term communication channel refers to a conduit for an information exchange between the mobile devices, and the term communication session refers to the information interchange, with the information interchange typically having a defined start and end.

The mobile devices are connectable to the mobile network in that, when the mobile devices are connected to the mobile network, mobile communication between the mobile devices can take place via the mobile network, e.g., via the base stations and the core nodes of the mobile network. The mobile devices are also arranged for establishing a D2D communication channel between the mobile devices so as to enable direct communication. The D2D communication may be established between two mobile devices. However, the D2D communication may equally involve a plurality of more than two mobile devices.

The D2D communication session is established, i.e., set up, in the following manner. First, an initiation key is preloaded on each of the mobile devices. Here, the term preloading refers to a loading of the initiation key on a mobile device before establishing the D2D communication session. For example, the initiation key may be loaded on the mobile device already before a request is received to establish the D2D communication session. The initiation key is used on each of the mobile devices in establishing the D2D communication session. Hence, when a request for establishing the D2D communication session is received, e.g., from the user or another mobile device, it is not necessary anymore to obtain the initiation key in order to establish the D2D communication session, i.e., it is already available on the mobile device.

The initiation key is used in establishing the D2D communication session in the following ways. The initiation key is associated with a validity period. The validity period is available to the mobile device, e.g., by being provided next to the initiation key, being derivable from the initiation key, etc. The validity period indicates a period in time in which the initiation key is deemed to be valid for use in establishing the D2D communication session. On each of the mobile devices which are to take part in the D2D communication session, a validity of the initiation key is verified based on the current time. This may be in response to a request to establish the D2D communication session. The current time is thus used to determine whether the initiation key is considered to be valid or not. If the initiation key is considered to be valid, e.g., due to the current time being in the validity period, the initiation key is used in performing a key agreement procedure between the mobile devices.

Here, the term key agreement procedure refers to a procedure which is performed between the mobile devices which results in a session key being agreed on, with the mobile devices each being able to influence the outcome of the procedure, i.e., the session key. The key agreement procedure is performed via the D2D communication channel, e.g., by exchanging messages between the mobile devices, with the messages together constituting

the key agreement procedure. The messages may be exchanged as part of an initial D2D communication session having been established over the D2D communication channel.

The key agreement procedure provides the session key based on whether the initiation key, as used by each respective mobile device in the key agreement procedure, matches. As such, a valid session key is obtained provided that each respective mobile device uses a same initiation key in the key agreement procedure. The session key constitutes a key used for cryptographically protecting messages in a communication session, such as confidentiality protection using encryption or integrity protection using message authentication codes. The D2D communication session is established using the session key. Thus, a D2D communication session is obtained in which messages, such as those of a voice or video transmission between the mobile devices, are cryptographically protected using the session key. The session key is used for a particular D2D communication session. Hence, in order to establish a new D2D communication session at a later moment in time, typically a new session key needs to be obtained or generated.

The above measures have the effect that a D2D communication session is established based on an initiation key. Here, the initiation key essentially functions as an authorization token in that a mobile device needs the initiation key to establish the D2D communication session. By providing an initiation key which is associated with a validity period and verifying the validity of the initiation key on the mobile device based on a current time, a time-based control mechanism is provided in that the initiation key is deemed valid only in a predetermined period and deemed invalid outside of said period.

The above measures offer control to the operator over the D2D communication in the following ways. By requiring a valid initiation key to establish the D2D communication session, the operator obtains control in that he can chose to whom the initiation key is provided, according to which conditions, etc. Moreover, by means of the validity period, the operator obtains time-based control, e.g., so as to prevent the re-use of old initiation keys. By using the initiation key in a key agreement procedure which is based on a match of the initiation keys used by the mobile devices, the operator obtains control in that not just any initiation key can be used in establishing the D2D communication session; rather, a success of the key agreement procedure depends on whether the initiation key, as used by each of the mobile devices in establishing the D2D communication session, matches.

Advantageously, by preloading the initiation key, the D2D communication session can be established under the operator's control even when one or more of the mobile devices are currently outside the operator's direct control, e.g., by being outside a range of

the mobile network. Advantageously, the mobile devices can autonomously establish the D2D communication session, i.e., without a need for contacting 3rd parties.

Optionally, the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network. Preloading the initiation key via the mobile network is convenient as mobile devices are frequently connected to the mobile network and thus no additional means is needed for preloading the initiation key. Advantageously, the mobile network provides a secure channel for preloading the initiation key. Advantageously, the initiation key can be automatically preloaded, i.e., without requiring user actions.

Optionally, the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device. The initiation key is thus stored such that it cannot be easily read by, e.g., the user or an application running on the mobile device. Advantageously, a tampering with the initiation key is made more difficult.

Optionally, the secure storage area is provided by a trusted computing subsystem of each respective mobile device. Here, the mobile device comprises, either as an integral part or as a removable part, a trusted computing subsystem. Such a trusted computing subsystem may be used for performing computing steps on the mobile device which require a certain level of security, such as authenticating the mobile device on the mobile network. An example of a removable trusted computing subsystem is a so-termed Universal Integrated Circuit Card (UICC) which may, in turn, comprise a Universal Subscriber Identity Module (USIM) application for use in authenticating the mobile device on the mobile network. The secure storage area provided by such a trusted computing subsystem, e.g., the memory of the UICC, is well suited for securely storing the initiation key on the mobile device.

Optionally, at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem. Hence, the use of the initiation key outside of the secure storage area provided by the trusted computing subsystem is reduced or avoided. Advantageously, a tampering with the initiation key is made more difficult.

Optionally, the method further comprises:

- preloading a set of initiation keys on each of the mobile devices, the set of initiation keys key being associated with a respective set of validity periods; and
- performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.

As such, each of the mobile devices is provided with multiple different initiation keys. To enable a same initiation key being used by each of the mobile devices in establishing the D2D communication session, a key synchronization procedure is performed in which it is identified which initiation key is available to all or most of the mobile devices, with said initiation key being selected for use in establishing the D2D communication session. Advantageously, a suitable initiation key can be conveniently established. Advantageously, the key synchronization procedure provides feedback if a mobile device does not have a suitable initiation key before performing the key agreement procedure.

Optionally, the method further comprises:

- preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys; and
- performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.

By performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers, it is not needed to involve the initiation keys themselves in the key synchronization procedure, e.g., by exchanging the initiation keys over the D2D communication channel. Advantageously, a tampering with the initiation keys is made more difficult since only the key identifiers are exchanged. Nevertheless, a tampering of the key identifiers, e.g., so as to feign a matching of initiation keys, will still fail as the key agreement procedure only provides the session key if the actual initiation keys match.

Optionally, the method further comprises disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session. Thus, an initiation key can only be used once in establishing a D2D communication session. For establishing a new D2D communication session, a new initiation key is needed. Advantageously, the operator obtains control over a number of times that a D2D communication session can be established, e.g., for limiting said number of times.

Optionally, the set of validity periods is constituted at least in part by different but overlapping validity periods. The different but overlapping validity periods together constitute a larger period in time. Since the validity periods overlap, there are no gaps in the larger period in time. The different but overlapping validity periods are associated with initiation keys. As a result, at any point in time in the larger period, an initiation key is available that can be validly used in establishing the D2D communication session.

Optionally, the initiation key is associated with a virtual network identity, and the verifying the validity of the initiation key further comprises determining a match of the

virtual network identity on each of the mobile devices via the D2D communication channel. Thus, the D2D communication session can only be established between mobile devices that have a same virtual network identity. Advantageously, the operator can set up a virtual network of mobile devices between which D2D communication is possible, while preventing D2D communication with mobile devices outside of said virtual network or between mobile devices belonging to different virtual networks.

Optionally, the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and the verifying the validity of the initiation key is further based on the usage count. Advantageously, the operator obtains control over a number of times that a D2D communication session can be established. Advantageously, said control can be provided with one initiation key, e.g., a master key, which can be used for establishing multiple D2D communication sessions. Thus, it is not needed to provide a set of initiation keys which each can only be used once for establishing a D2D communication session.

Optionally, the method further comprises adjusting the usage count after use of the initiation key in establishing the D2D communication session. Hence, a use of the initiation key in establishing a D2D communication session is reflected in the usage count.

Optionally, the method further comprises requesting a further initiation key via the mobile network if i) no initiation key is deemed valid, or ii) the key agreement procedure fails in providing the session key.

Optionally, the key agreement procedure comprises:

- a three-pass authentication procedure; or
- a use of the initiation key to encrypt a message exchange

between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.

Modifications and variations of the control software, the mobile device and the mobile network, which correspond to the described modifications and variations of the method, can be carried out by a person skilled in the art based on the present description.

The invention is defined in the independent claims. Advantageous yet optional embodiments are defined in the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter. In the drawings,

Fig. 1 shows mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network;

Fig. 2 shows a method for establishing a D2D communication session between the mobile devices;

Fig. 3 shows a mobile device comprising a mobile subsystem and a computing subsystem, the computing subsystem comprising a storage area;

Fig. 4 shows a determining a match of a virtual network identity on each of the mobile devices via the D2D communication channel;

Fig. 5 shows a performing a key synchronization procedure between the mobile devices over the D2D communication channel;

Fig. 6 shows a key agreement procedure being initialized over the D2D communication channel by using an initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret;

Fig. 7 shows a key agreement procedure being performed over the D2D communication channel, being based on a three-pass authentication procedure; and

Fig. 8 shows another key agreement procedure being performed over the D2D communication channel in which identifiers identifying the mobile devices are encrypted.

It should be noted that items which have the same reference numbers in different Figures, have the same structural features and the same functions, or are the same signals. Where the function and/or structure of such an item has been explained, there is no necessity for repeated explanation thereof in the detailed description.

DETAILED DESCRIPTION OF EMBODIMENTS

Fig. 1 shows a first mobile device MD1 and a second mobile device MD2, henceforth also jointly referred to as mobile devices MD. The mobile devices MD are individually connectable to a mobile network MN. This is illustrated in Fig. 1 by a communication channel existing between each mobile device MD and the mobile network MN, i.e., a device-to-network communication channel DNC. The mobile network MN is shown to comprise base-stations BS1, BS2. In this particular example, each of the mobile devices MD is connected to a different one of the base-station BS1, BS2. The base-stations BS1, BS2 are mutually connected via core nodes CN of the mobile network. As such, when the mobile devices MD are connected to the mobile network MN, communication between the mobile devices MD can take place via the mobile network MN in that an information

interchange can be performed via a first one of the base-stations BS1, the core nodes CN, and a second one of the base-stations BS2 of the mobile network MN, or vice versa.

The mobile devices MD are also mutually connectable via a D2D communication channel DDC. The D2D communication channel DDC may have been established or setup using a mobile subsystem MS1, MS2 of each respective mobile device MD1, MD2. The present invention involves establishing a D2D communication session between the mobile devices MD over the D2D communication channel DDC.

The D2D communication session may be established in accordance with the method 100 as shown in Fig. 2. The method 100 comprises firstly preloading 120 an initiation key on each of the mobile devices MD. The preloading 120 may be performed using the mobile network MN. For that purpose, the mobile network MN may be arranged for, when one of the mobile devices MD is connected to the mobile network MN, providing the initiation key to said mobile device MD via the device-to-network communication channel DNC. However, the preloading 120 may also involve another communication channel, and in particular a secure communication channel. For example, the initiation key may be preloaded using Near Field Communication (NFC), e.g., at a physical point of sale, or using Wi-Fi, e.g., via a Wireless Local Area Network (WLAN).

Although not shown in Fig. 1, each mobile device MD may comprise a storage area for storing the initiation key on the respective mobile device MD. Consequently, the step of preloading 120 the initiation key on each of the mobile devices MD may comprise storing the initiation key in the storage area of the respective mobile device MD.

The initiation key is associated with a validity period. The method 100 further comprises, on each of the mobile devices MD, verifying 140 a validity of the initiation key based on a current time. For that purpose, each mobile device MD1, MD2 comprises a computing subsystem CS1, CS2 which is arranged for performing said step and which may have knowledge of the current time or be arranged for obtaining the current time. It is noted that the validity period may be expressed in any suitable time-based quantity, e.g., a day, an hour of a day, a minute of an hour, etc. Consequently, the term current time may refer to, e.g., a current day and/or a current time of the day. Hence, verifying the validity of the initiation key may comprise determining whether the current day falls within the validity period, and if so, whether the current day is either a first day or a last day of the validity period, and if so, whether the current time of the day falls within the validity period.

The method 100 further comprises, on each of the mobile devices MD, if the initiation key is deemed valid, generating 160 a session key using the initiation key by using

the initiation key in performing a key agreement procedure between the mobile devices MD over the D2D communication channel DDC. The computing subsystem CS1, CS2 of each mobile device MD is arranged for performing said step, while involving the mobile subsystem MS1, MS2 to carry out an actual message exchange over the D2D communication channel DDC.

The key agreement procedure is arranged for resulting in the session key if the initiation key used by each of the mobile devices MD matches. Having obtained the session key, the method 100 comprises, on each of the mobile devices MD, establishing 180 the D2D communication session over the D2D communication channel DDC based on the session key. The mobile subsystem MS1, MS2 of each mobile device MD is arranged for performing said step using the session key obtained from the computing subsystem CS1, CS2.

Although not shown in Fig. 2, control software may be provided comprising instructions for, upon execution of the control software on a mobile device, causing the mobile device to establish the D2D communication session according to the method 100 as shown in Fig. 2, i.e., by verifying 140 a validity of the initiation key based on a current time, generating 160 a session key using the initiation key, and establishing 180 the D2D communication session over the D2D communication channel based on the session key.

Fig. 3 shows the first mobile device MD1 in more detail, with the first mobile device MD1 here being exemplary of each of the mobile devices MD. The first mobile device MD1 comprises a mobile subsystem MS1 and a computing subsystem CS1 as introduced earlier in reference to Figs. 1 and 2. Here, the term mobile subsystem refers to a subsystem of the mobile device that performs and/or enables the main functionality of the mobile device, including establishing a communication channel, exchanging messages over the established communication channel, performing various computing functions, etc. An example of a mobile subsystem is a mobile System on a Chip (SoC) comprising an application processor, a display processor, one or more modems, an integrated LTE radio. Another example is said mobile SoC and an external LTE radio which is connected to the mobile SoC.

Fig. 3 shows the first mobile device MD1 comprising a storage area SA1 for storing the initiation key as provided during the preloading procedure. The storage area SA1 may be a secure storage area. In the example of Fig. 3, the storage area SA1 is provided by the computing subsystem CS1. The computing subsystem CS1 may be a trusted computing subsystem, thereby automatically providing a secure storage area. Such a trusted computing subsystem CS1 may be constituted by a UICC which comprises a USIM application. The USIM application may be arranged for establish the D2D communication session according

to the method 100 as shown in Fig. 2. The interface to and from the UICC may be protected by means of secure channel protocol, e.g., according to the ETSI TS 102 484 technical specification, so as to make eavesdropping and tampering more difficult.

In the following, two detailed embodiment of the present invention are presented which each comprise various advantageous yet optional measures. It will be appreciated that those measures may also be combined and/or individually applied to the general concept of the present invention, unless prevented by technical incompatibilities.

The first detailed embodiment comprises preloading a set of initiation keys on each of the mobile devices MD, the set of initiation keys key being associated with a respective set of validity periods. For that purpose, the mobile network MN may send one or more messages to the computing subsystem CS1, CS2 of each mobile device MD1, MD2 via each respective mobile subsystem MS1, MS2. The one or more messages may comprise the set of initiation keys and the set of validity periods. In addition, the one or more messages may comprise a current network time and/or a set of limitations. In addition to the set of initiation keys and the set of validity periods, the one or messages may comprise a set of key identifiers, each of the set of key identifiers identifying a respective one of the set of initiation keys. In addition to the set of initiation keys and the set of validity periods, the one or more messages may comprise a set of virtual network identities, each of the set of virtual network identities being associated with a respective one of the set of initiation keys.

The following table shows an example of the information which may be preloaded on a mobile device:

Virtual Network Id	**Key Id**	**Initiation key**	**Valid from (hh:mm dd:mm:yyyy)**	**Valid Through (hh:mm dd:mm:yyyy)**
Corporation X	102	Secret123	11:00 01/01/2012	13:00 02/01/2012
Corporation X	103	Geheim123	11:00 01/01/2012	13:00 02/01/2012
Corporation X	104	gEHEIM321	11:00 01/01/2012	13:00 02/01/2012
Corporation X	105	SeCRet123	11:00 02/01/2012	13:00 03/01/2012
Corporation X	106	GeHEim123	11:00 02/01/2012	13:00 03/01/2012
Corporation X	107	sEcrET321	11:00 02/01/2012	13:00 03/01/2012
Operator Y	53	sECRET321	00:00 01/12/2011	03:00 01/01/2012
Operator Y	54	123secret	00:00 01/12/2011	03:00 01/01/2012

Operator Y	55	sECRet321	00:00 01/01/2012	03:00 01/02/2012
Operator Y	56	123seCRet	00:00 01/01/2012	03:00 01/02/2012

In general, as is the case in the above example, the set of validity periods may be constituted at least in part by different but overlapping validity periods.

Each computing subsystem CS1, CS2 may store the set of initiation keys, the set of key identifiers and the current network time in a secure storage area SA1 of the computing subsystem. Each computing subsystem CS1, CS2 may also dispose of any initiation keys already stored which have expired according to the current network time. The set of virtual network identities may be stored elsewhere in each of the mobile devices MD1, MD2, i.e., may not need to be stored in the computing subsystem CS1, CS2.

As part of establishing the D2D communication session over the D2D communication channel DDC, it may be determined whether a virtual network identity on each of the mobile devices MD matches. This allows enabling D2D communication sessions to be established between mobile devices MD which share a virtual network identity, whilst preventing D2D communication sessions from being established between mobile devices MD which do not share a virtual network identity. For example, a corporate mobile device may comprise a virtual network identity of the corporation as well as a virtual network identity of the operator's own virtual network. The latter may allow users to establish a D2D communication session with other users of the operator's mobile network. In general, virtual network identities may be provided for, e.g., a certain locality, certain group of users, companies, families, etc. A virtual network identity may also be provided that allows cross-operator D2D communication sessions to be established, i.e., between mobile devices which normally belong to mobile networks that are operated by different operators.

Fig. 4 shows an example 142 of how a match of a virtual network identity on each of the mobile devices MD may be determined via the D2D communication channel DDC. Here, the computing subsystem CS1 and mobile subsystem MS1 of the first mobile device MD1 are schematically shown on a left-hand side, and the computing subsystem CS2 and mobile subsystem MS2 of the second mobile device MD2 are shown on a right hand side. Furthermore, a message exchange between the mobile devices MD1, MD2 via the D2D communication channel DDC is show schematically over time by means of arrows which indicate a source and destination of the message. Moreover, rounded rectangles are used to indicate steps being performed by either of the mobile devices MD1, MD2, with a horizontal position of a rectangle indicating on which subsystem the step is performed.

A match of the virtual network identity may be determined as follows. Firstly, the first mobile device MD1 sends a message to the second mobile device MD2 over the D2D communication channel, the message comprising many or all of the virtual network identities which are stored on the first mobile device MD1. In response, in a step titled DET_OVERLAP_STEP, the second mobile device MD2 determines which of the virtual network identities of the first mobile device MD1 overlap with those stored locally, i.e., on the second mobile device MD2. Moreover, in a step titled ORDER_STEP, the overlapping virtual network identities are ordered according to a priority list of the second mobile device MD2, and a result thereof is sent by message to the first mobile device MD1. Upon receipt, in a step titled SELECT_STEP, the overlapping virtual network identities are also ordered according to a priority list of the first mobile device MD1, and one of the overlapping virtual network identities is selected which ranks highest when combining both priority lists. Finally, the selected virtual network identity is sent by message to the second mobile device MD2, which in turn acknowledges the selected virtual network identity by return message.

The verifying the validity of the initiation key may comprise the aforementioned determining of the match of the virtual network identity on each of the mobile devices via the D2D communication channel. Consequently, if no matching virtual network identity can be found, the initiation keys on both mobile devices may be considered invalid for the purpose of establishing a D2D communication session between the mobile devices MD since said keys are associated with non-matching virtual network identities.

Having verified the match of the virtual network identity, the establishing of the D2D communication session may continue as follows. Each of the mobile devices MD1, MD2 may be arranged for performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key. Fig. 5 shows an example 162 of such a key synchronization procedure. This particular example is based on an exchange of one or more of the set of key identifiers between the mobile devices MD1, MD2. Here, upon request from the mobile subsystem MS1, the computing subsystem CS1 searches for a key identifier which is associated with a valid initiation key, meaning that said initiation key is valid at the current time and has not been used before in establishing a D2D communication session. The computing subsystem CS1 may search for the key identifier based on various criteria, such as, e.g., whether a key identifier is valid at the current time and a reasonable period in the future, e.g., the next 15 minutes. The search may also be based on a key sequence number associated with each of the key identifiers, with the computing

subsystem CS1 selecting one of the key identifiers that is associated with a lowest key sequence number. In case the key identifiers are numerical, the computing subsystem CS1 may also select a lowest one of the key identifiers. In case the key identifiers are sequentially ordered, the computing subsystem CS1 may also select a first or last one of the key identifiers. It will be appreciated that various criteria such as the above may be combined.

The computing subsystem CS1 sends the key identifier KeyID which was found to the mobile subsystem MS1, which in turn sends it to the second mobile device MD2. On the second mobile device MD2, the mobile subsystem MS2 forwards the key identifier KeyID to the computing subsystem CS2. Moreover, the second mobile device MD2 also performs a same process, either in parallel or after receiving the key identifier KeyID from the first mobile device MD1. As a result, the computing subsystems CS1, CS2 on each mobile device MD1, MD2 comprise both key identifiers. Each computing subsystem CS1, CS2 then selects, in a step titled MAX_KEYID_STEP, the key identifier which is highest, thereby also selecting the initiation key which is identified by said key identifier.

It is noted that, in general, initiation keys may be disabled or removed after use in establishing a D2D communication session. In this case, however, certain types of key synchronization procedures, such as the example shown in Fig. 5, may lead to a rapid consumption of initiation keys. Alternatively, the first mobile device MD1 may send the key identifier to the second mobile device MD2. The second mobile device MD2 may request its computing subsystem CS2 to determine if it comprises a valid initiation key associated with this key identifier. If so, the initiation key may be directly selected. If not, the computing subsystem CS2 may search for a lowest key identifier which is associated with a valid initiation key, and return the found key identifier to the mobile subsystem MS2 for sending to the first mobile device MD1. Upon receipt, the first mobile device MD1 may request its computing subsystem CS1 to determine if it comprises a valid initiation key associated with this key identifier. If so, the initiation key may be directly selected. If not, the computing subsystem CS1 may search for a lowest key identifier and again repeat the above process.

It is noted that the above alternative key synchronization procedure may be repeated several times. Alternatively, the key synchronization procedure may be based on an exchange of many or all key identifiers available to each respective mobile device so as to more rapidly determine a key identifier that identifies a matching and valid initiation key.

It is further noted that the key exchange procedure may be combined with an authentication procedure. The authentication procedure may be a prerequisite part of the setup of the D2D communication session. As a result, messages which are exchanged

between the mobile devices may serve both for the purpose of authentication as well as for key exchange. Figs. 7 and 8 show an example of this. For example, a message may constitute a challenge response from one mobile device while at the same time being part of the key exchange procedure between the mobile devices.

Having selected a matching one of the set of initiation keys on each of the mobile devices as the initiation key, the establishing of the D2D communication session may continue by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel. Fig. 6 shows an example 164 of a first part of such a key agreement procedure, which comprises using the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret. This first part of the key agreement procedure may be used to initialize a key exchange procedure based on the shared secret. Essentially, the first part of the key agreement procedure may be considered as a bootstrapping of the subsequent key exchange. An example of such a key exchange procedure is the Diffie-Hellman key exchange as known from the field of cryptography.

In the example of Fig. 6, each of the computing subsystems CS1, CS2 retrieves the initiation key from the storage area. In a step titled ENC_SECRET1_STEP, the computing subsystem CS1 of the first mobile device MD1 creates a message which comprises a secret, i.e., secret1, encrypted with the initiation key. The message is forwarded to the mobile subsystem MS1 which in turn sends the message to the second mobile device MD2. Here, the mobile subsystem MS2 forwards the message to the computing subsystem CS2. In a step titled DEC_SECRET1_STEP, the computing subsystem CS2 decrypts the message with the initiation key. In a step titled ENC_SECRET2_STEP, the computing subsystem CS2 creates a message with another secret, i.e., secret 2, encrypted with the initiation key. Moreover, in a step titled CALC_SK_STEP, a session key SK is calculated based on the combination of both secrets, i.e., secret1 and secret2, and included in the message. The message is sent back by the second mobile device MD2 to the first mobile device MD1. Here, the mobile subsystem MS1 forwards the message to the computing subsystem CS1. In a step titled DEC_SECRET2_STEP, the computing subsystem CS1 decrypts the message with the initiation key. In a step titled CALC_SK_STEP, the session key SK is calculated based on the combination of both secrets. As a result, on each of the computing subsystems CS1, CS2, both secrets are available, i.e., secret1 and secret2, thus allowing the respective computing subsystems to calculate a same session key SK.

It is noted that instead of the example of Fig. 6, various alternative mechanisms may be used as well for obtaining the shared secret. For example, one of the

point-to-point key establishment mechanisms as described in the ISO/IEC 11770-2 standard may be used. For example, the key establishment mechanism 5 as described in section 6.5 of said document may be used.

As a result of the subsequent key exchange procedure, a session key is obtained on each of the mobile devices MD1, MD2. This allows the D2D communication session to be established over the D2D communication channel based on the session key.

A second detailed embodiment comprises preloading a so-termed master key on each of the mobile devices MD1, MD2. Here, the term master key refers to an initiation key which is combined with a usage count so as to allow multiple D2D communication sessions to be established using one initiation key. The initiation key and the usage count constitute an alternative to the preloading of a plurality of initiation keys which may each be used only once in establishing a D2D communication session. It is noted that the initiation key may constitute a master key in that, each time an initiation key is needed for establishing a particular D2D communication session, a temporary initiation key is derived from the master key for that purpose. Hence, the initiation key may be used multiple times to establish a temporary initiation key for use in a particular D2D communication session. The mobile network MN may provide the computing subsystem CS1, CS2 of each mobile device MD1, MD2 with such an initiation key, the initiation key being valid for a particular validity period. Moreover, the mobile network MN may provide or set the usage count. The usage count may represent, e.g., a number of time the computing subsystem is allowed to generate a session key using the initiation key. The mobile network MN may also periodically provide the current network time so as to enable each computing subsystem CS1, CS2 to dispose of any initiation keys stored in the computing subsystem which have already expired according to the current network time. Additionally or alternatively, the mobile network MN may provide the current network time when preloading an initiation key on a mobile device MD1, MD2.

After having possibly verified a match of a virtual network identity, the validity of the initiation key is verified based on a current time and the usage count, and if the initiation key is deemed valid, the initiation key is used in performing a key agreement procedure between the mobile devices over the D2D communication channel. An example 166 of this is shown in Fig. 7, where the key agreement procedure is shown which is based on a three-pass authentication procedure, as specified by, e.g., the ISO/IEC 9798-4 standard.

Initially, each computing subsystems CS1, CS2 provides an identifier, i.e., ID1 and ID2, respectively, to each respective mobile subsystem MS1, MS2. Each identifier ID1, ID2, identifies the respective mobile device MD1, MD2. The identification may be

indirect in that each identifier ID1, ID2 may identify the respective computing subsystem CS1, CS2, which in turn allows the mobile device MD1, MD2 to be identified since the computing subsystem CS1, CS2 is an integral or removable part of the mobile device.

The further steps shown in Fig. 7 may be explained as follows. Here, the numerals correspond to those shown in Fig. 7.

1. The first mobile device MD1, being in this example the mobile device initiating the key agreement procedure, requests the computing subsystem CS1 to provide an key identifier KeyID which identifies an initiation key that is valid at the current time. The computing subsystem CS1 determines, in a step titled SELECT_KEYID_STEP, whether it comprises such an initiation key and if so, whether usage of the initiation key is still allowed, e.g., by checking whether the usage count is still below a given threshold in case the usage count corresponds to a number of uses, or whether the usage count is still above zero in case the usage count corresponds to a number of remaining uses. If this is the case, the initiation key is considered to be valid, and the computing subsystem CS1 establishes a key identifier KeyID identifying the initiation key. Moreover, the computing subsystem CS1 generates a random RND1, the random RND1 constituting a challenge in the authentication of the computing subsystem CS2 of the second mobile device MD2.

2. The computing subsystem CS1 provides the key identifier KeyID and the random RND1 to the mobile subsystem MS1 of the first mobile device MD1.

3. The first mobile device MD1 sends the key identifier KeyID, the random RND1 and the identifier ID1 to the second mobile device MD2 over the D2D communication channel DDC so as to initialize the key agreement procedure.

4. In response, the second mobile device MD2 requests its computing subsystem CS2 to initiate the key agreement procedure. For that purpose, it provides the key identifier KeyID, the random RND1 and the identifier ID1 to the computing subsystem CS2. In addition, the computing subsystem CS2 may request the second mobile device MD2 to provide the current time so as to enable the computing subsystem CS2 to verify if the initiation key identified by the key identifier KeyID is valid for the current time. This constitutes an additional verification step on the receiving, i.e., non-initializing, end of the key agreement procedure. When the initiation key identified by the key identifier KeyID is available to the computing subsystem CS2 and if usage of the initiation key is still allowed, e.g., in case its usage count is still above zero, the computing subsystem CS2 generates, in a step titled CALC_RESP1_STEP, a random RND2 and a session key SK_A for the authentication. The computing subsystem CS2 further calculates a response to the challenge

from the first mobile device MD1, being indicated as $E\_SK_A(X)$ with X = RND1 || RND2 || ID2. Here, the E_SK_A denotes an encryption function that uses SK_A as the session key and X as the message. An example of such a function is a Message Authentication Code (MAC).

5. The computing subsystem CS2 provides $E\_SK_A(X)$ and the random RND2 to the mobile subsystem MS2 of the second mobile device MD2.

6. The second mobile device MD2 sends $E\_SK_A(X)$, the random RND2 and the identifier ID2 to the first mobile device MD1, constituting a response to step 3.

7. The first mobile device MD1 requests its computing subsystem CS1 to authenticate the response received from the second mobile device MD2 and to generate a response to the challenge provided in the form of RND2.

8. In a step titled CALC_RESP2_STEP, the computing subsystem CS1 generates a session key for authentication of SK_A, and checks the response $E\_SK_A(X)$ from the second mobile device MD2. The computing subsystem CS1 then calculates a response to the challenge from the second mobile device MD2, being indicated by $E\_SK_A(Y)$ with Y = RND2 || RND1 || ID1. The computing subsystem CS1 generate a session key for use in the D2D communication session SK_C, and optionally a session key for integrity protection SK_I. The computing subsystem CS1 may then adjust, e.g., decrease, the usage count of the initiation key. Finally, the computing subsystem CS1 provides $E\_SK_A(Y)$, the session key SK_C, and optionally SK_I, to the mobile subsystem MS1.

9. The first mobile device MD1 sends a response to the challenge from the second mobile device MD2 in the form of $E\_SK_A(Y)$ to the second mobile device MD2.

10. In response, the second mobile device MD2 requests its computing subsystem CS2 to check, i.e., authenticate, $E\_SK_A(Y)$.

11. The computing subsystem CS2 then determines, in a step titled CALC_SESSIONKEY_STEP, if $E\_SK_A(Y)$ is valid, and if so generates the session key SK_C, and optionally SK_I, and provides both to the mobile subsystem MS2. The computing subsystem CS2 may then adjust, e.g., decrease, the usage count of the initiation key.

12. The mobile subsystem MS2 of the second mobile device MD2 establishes the D2D communication session with the mobile subsystem MS1 of the first mobile device MD1 using the session key SK_C. Hence, a secure D2D communication session is obtained.

Fig. 8 shows an alternative 168 to the key agreement procedure 166 as shown in Fig. 7. A difference concerns that here, the identifiers ID1 and ID2 are encrypted during exchange, whereas in the key agreement procedure of Fig. 7, the identifiers ID1 and ID2 were exchanged without being encrypted. By encrypting the identifiers ID1 and ID2 during

exchange, it may be prevented that users are tracked and/or identified through eavesdropping of the message exchange between the mobile devices MD1, MD2.

The further steps shown in Fig. 8 may be explained as follows. Here, the numerals correspond to those shown in Fig. 8.

1. Step 1 corresponds to step 1 as discussed in reference to Fig. 7, with the addition that the computing subsystem CS1 generates a challenge, being essentially a message that is encrypted using the initiation key, the encrypted message being denoted by E_MK, and the encrypted message comprising the random RND1 and the identifier ID1.

2. The computing subsystem CS1 provides the key identifier KeyID and the challenge to the mobile subsystem MS1 of the first mobile device MD1.

3. The first mobile device MD1 sends the key identifier KeyID, the challenge to the second mobile device MD2 over the D2D communication channel DDC so as to initialize the key agreement procedure.

4. In response, the second mobile device MD2 requests its computing subsystem CS2 to initiate the key agreement procedure. For that purpose, it provides the key identifier KeyID, the challenge to the computing subsystem CS2. In addition, the computing subsystem CS2 may request the second mobile device MD2 to provide the current time so as to enable the computing subsystem CS2 to verify if the initiation key identified by the key identifier KeyID is valid for the current time. This constitutes an additional verification step on the receiving, i.e., non-initializing, end of the key agreement procedure. When the initiation key identified by the key identifier KeyID is available to the computing subsystem CS2 and if usage of the initiation key is still allowed, e.g., in case its usage count is still above zero, the computing subsystem CS2 generates, in a step titled CALC_RESP1_STEP, a random RND2 and a session key SKA for the authentication. The computing subsystem CS2 further calculates a response to the challenge from the first mobile device MD1, being indicated as E_SKA(X) with X = RND1 || RND2 || ID2. Here, the E_SKA denotes an encryption function that uses SKA as the session key and X as the message. An example of such a function is a Message Authentication Code (MAC). The computing subsystem CS2 also calculates a challenge, E_MK(RND2||ID2), for which the same E_MK is used that the computing subsystem CS1 of the first mobile device MD1 used in its challenge.

5. The computing subsystem CS2 provides E_SKA(X) and the challenge to the mobile subsystem MS2 of the second mobile device MD2.

6. The second mobile device MD2 sends E_SKA(X) and the challenge to the first mobile device MD1, constituting a response to step 3.

7. The first mobile device MD1 requests its computing subsystem CS1 to authenticate the response received from the second mobile device MD2 and to generate a response to the challenge provided in the form of E_MK(RND2||ID2).

8-12. Steps 8-12 correspond to steps 8-12 as discussed in reference to Fig. 7.

It is noted that in general, a computing subsystem of a mobile device may request a further initiation key via the mobile network if i) no initiation key is deemed valid, or ii) the key agreement procedure fails in providing the session key.

It will be appreciated that the present invention may be advantageously applied to Direct LTE, i.e., LTE-based D2D communication between mobile devices. In particular, the present invention allows the following advantageous uses.

Corporation X has purchased a direct mode subscription from operator Y for all its employees. As a result, for example once a week during the night or during low network load, all mobile devices of the corporation, such as mobile phones and dongles, are provided with a set of a hundred initiation keys which are valid for every day of the following week. On a next Monday, several employees have a meeting in which they would like to share a presentation. However, they are located in a meeting room without network coverage, i.e., are outside a range of the mobile network. They plug-in their dongles into their laptops and setup an ad hoc network based on Direct LTE. Since all dongles were provided with a same set of initiation keys, the employees are able to setup a LTE-based D2D communication session in the meeting room without needing to access the mobile network.

Another advantageous use may be the following. Again, corporation X has purchased a direct mode subscription. Again, for example once a week during the night or during low network load, all mobile devices of the corporation are provided with a set of a hundred initiation keys which are valid for every day of the following week. However, one dongle was turned off during said preloading procedure. On a next Monday, several employees have a meeting in which they would like to share a presentation. They are located in a room with network coverage. They plug-in their dongles into their laptops and setup an ad hoc network based on Direct LTE. Because most of the dongles were provided with a same set of initiation keys, the employees are able to setup a LTE-based D2D communication session in the meeting room without needing to access the mobile network. However, the dongle which was turned off during the preloading procedure can still join the D2D communication session by requesting from the mobile network the set of initiation keys, and once said set has been provided, the dongle joins the D2D communication session.

Another advantageous use may be the following, which is a same as the aforementioned use, except that the employees are located in a room with network coverage. They plug-in their dongles into their laptops and setup an ad hoc network based on Direct LTE. Some dongles already have keys available for the D2D communication session, but some only have expired keys, e.g., because D2D communication hasn't been used for some time and therefore no initiation keys needed to be preloaded or updated. All dongles now request from the mobile network a set of initiation keys and once said set has been provided, each dongle joins the D2D communication session. Later that day, the employees meet again. Now, a D2D communication session can be established immediately, i.e., without a need to contact the mobile network, since the dongles now already have a set of valid initiation keys.

Yet another advantageous use may the following. For emergency services, it is of utmost importance to be able to communicate at all times. Hence, a mobile device which relies on network coverage to establish a D2D communication session may not be desirable. This may be avoided by preloading initiation keys frequently, e.g., every time when a mobile device is switched on, and/or by preloading initiation keys which are associated with a validity period that is relatively long. The preloading may also occur every night, when all the mobile devices are at a central location. During the day, the firefighters, policemen and ambulance personnel can choose direct mode operation in case network reception is inadequate, thereby still allowing communication amongst said emergency service personnel.

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative embodiments.

In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. Use of the verb "comprise" and its conjugations does not exclude the presence of elements or steps other than those stated in a claim. The article "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. The invention may be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In the device claim enumerating several means, several of these means may be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** February 27, 2015 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000	U.S. NATIONAL STAGE OF APPLICATION NO. PCT/EP2013/067904	
	FIRST NAMED INVENTOR Antonius Norp	FILING DATE August 29, 2013	
	EXAMINER	CONFIRMATION NO.	GROUP

U.S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Number-Kind Code (if known)	ISSUE DATE / PUBLICATION DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
	1.	2007/0253376 A1	11-01-2007	Bonta, et al.
	2.			
	3.			
	4.			
	5.			
	6.			
	7.			
	8.			
	9.			
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			

Copies of issued U.S. Patents and Published U.S. Applications are not required and are not being provided. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.

EXAMINER	DATE CONSIDERED

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** February 27, 2015 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000		U.S. NATIONAL STAGE OF APPLICATION NO. PCT/EP2013/067904
	FIRST NAMED INVENTOR Antonius Norp		FILING DATE August 29, 2013
	EXAMINER	CONFIRMATION NO.	GROUP

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	DOCUMENT NUMBER Country Code-Number-Kind Code (if known)	DATE MM-DD-YYYY	NAME OF PATENTEE OR APPLICANT OF CITED DOCUMENT
	1.	WO 2010/030515 A2	03-18-2010	QUALCOMM Incorporated
	2.	WO 2011/117677 A1	09-29-2011	Nokia, Inc.
	3.			
	4.			
	5.			
	6.			
	7.			
	8.			
	9.			
	10.			
	11.			
	12.			
	13.			
	14.			
	15.			
	16.			
	17.			
	18.			
	19.			
	20.			

EXAMINER	DATE CONSIDERED

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT IN AN APPLICATION** **LISTING OF REFERENCES** February 27, 2015 (Use several sheets if necessary)	ATTORNEY DOCKET NO. 4965.1017-000		U.S. NATIONAL STAGE OF APPLICATION NO. PCT/EP2013/067904
	FIRST NAMED INVENTOR Antonius Norp		FILING DATE August 29, 2013
	EXAMINER	CONFIRMATION NO.	GROUP

Examiner's Initials	Cite No.	**OTHER DOCUMENTS** *(Including Author, Title, Date, Pertinent Pages, Etc.)*
	1.	Fodor, G., et al., "Design Aspects of Network Assisted Device-to-Device Communications," *IEEE Communications Magazine*, pp. 170-177, March 2012.
	2.	Notification of Transmittal of The International Search Report and The Written Opinion of the International Searching Authority, PCT/EP2013/067904, date of mailing October 7, 2013.
	3.	
	4.	
	5.	
	6.	
	7.	
	8.	
	9.	
	10.	
	11.	
	12.	
	13.	
	14.	
	15.	
	16.	
	17.	
	18.	
	19.	

***Copies of any U.S. Office Communications or non-published U.S. Patent Applications are not being provided because the examiner has access to such documents through PAIR. We are not listing separately any prior U.S. Patent Office communications regarding the cited documents because the Examiner has access to any such actions through PAIR.**

EXAMINER	DATE CONSIDERED

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2010 (18.03.2010)

PCT

(10) International Publication Number
WO 2010/030515 A2

(51) International Patent Classification:
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/US2009/055262

(22) International Filing Date:
27 August 2009 (27.08.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/209,440 12 September 2008 (12.09.2008) US

(71) Applicant *(for all designated States except US)*: **QUALCOMM Incorporated** [US/US]; ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VANDERVEEN, Michaela** [US/US]; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **TSIRTSIS, Georgios** [GB/GB]; Flat 1, 1 Alexandria Road, London Greater London W13 ONP (GB). **PARK, Vincent, D.** [US/US]; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **CORSON, Mathew, Scott** [US/US]; 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(74) Agent: **O'HARE, James, K.**; ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(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,

[Continued on next page]

(54) Title: TICKET-BASED CONFIGURATION PARAMETERS VALIDATION

(57) Abstract: Aspects describe spectrum authorization, access control, and configuration parameters validation. Devices in an ad-hoc or peer-to-peer configuration can utilize a licensed spectrum if the devices are authorized to use the spectrum, which can be determined automatically. Aspects relate to distribution of authorization tickets by an authorization server as a result of validating a device's credentials and services to which the device is entitled. An exchange and verification of authorization tickets can be performed by devices as a condition for enabling a validated wireless link using the spectrum.

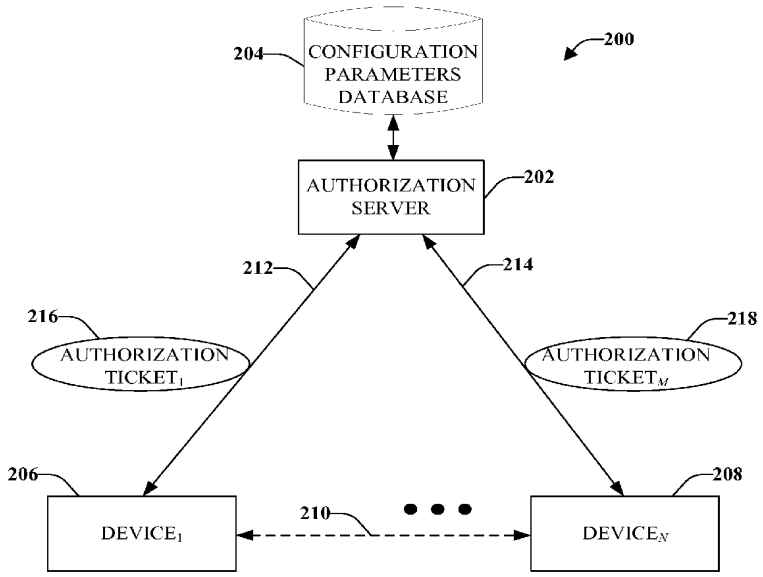


FIG. 2

WO 2010/030515 A2

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:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

TICKET-BASED CONFIGURATION PARAMETERS VALIDATION

BACKGROUND

I. Field

[0001] The following description relates generally to wireless communications and more particularly to authorizing communications over a licensed spectrum.

II. Background

[0002] Wireless communication systems are widely deployed to provide various types of communication and to transfer information regardless of where a user is located (inside or outside a structure) and whether a user is stationary or moving (*e.g.*, in a vehicle, walking). For example, voice, data, video and so forth can be provided through wireless communication systems. A typical wireless communication system, or network, can provide multiple users access to one or more shared resources. For instance, a system may use a variety of multiple access techniques such as Frequency Division Multiplexing (FDM), Time Division Multiplexing (TDM), Code Division Multiplexing (CDM), Orthogonal Frequency Division Multiplexing (OFDM), and others.

[0003] Generally, wireless communication networks are established through a device communicating with a base station or access point. The access point covers a geographic range or cell and, as the device is operated, the device can be moved in and out of these geographic cells.

[0004] A network can also be constructed utilizing solely peer-to-peer devices without utilizing access points or the network can include both access points and peer-to-peer devices. These types of networks are sometimes referred to as ad hoc networks. Ad hoc networks can be self-configuring whereby when a device (or access point) receives communication from another device, the other device is added to the network. As devices leave the area, they are dynamically removed from the network. Thus, the topography of the network can be constantly changing.

[0005] Ad-hoc networks enable communication devices to transmit and/or receive information while on the move. Communication is established using the spectrum, which is a valuable, limited resource comprising a broad range of electromagnetic radio frequencies utilized in the transmission of multiple types of data.

Ad-hoc networks may be communicatively coupled to other public or private networks, for example through wired and/or wireless access points, in order to enable the transfer of information to and from a device. Such ad-hoc networks typically include a multitude of devices communicating in a peer-to-peer manner. Ad-hoc networks may also include beacon points that emit strong signals to facilitate peer-to-peer communication amongst devices. For example, emitted beacons can contain timing information to aid in timing synchronization of such devices. These beacon points are positioned to provide wide area coverage as the device travels within and across different coverage areas.

[0006] If a communication system does not require operator-owned access points but utilizes a licensed spectrum belonging to a spectrum owner/licensee/provider, only authorized devices should be enabled to use the spectrum. In order for the spectrum owner/licensee to be reimbursed for the spectrum license fees, authorization for the spectrum is granted for devices associated with users or organizations that possess a business relationship with the spectrum provider or a broker representative thereof.

[0007] Thus, the spectrum provider can control use of its spectrum by employing an authorization server, which is a core network node or set of nodes that communicate with devices on a timeline or upon events as prescribed by user service agreements or by spectrum provider administration, in order to authenticate and authorize the devices to utilize the spectrum according to their service agreements.

[0008] Associated with ad-hoc communication using the spectrum is a series of configuration parameters necessary to properly make use of such links. These parameters are Internet Protocol (IP) addresses, upper-layer or network-layer identifiers, service identifiers, and the like. Misconfiguration of these parameters can result in security breaches. For example if a (misbehaving) device is able to utilize an IP address belonging to another network node as if that (stolen) IP address belongs to the misbehaving device, peers communicating with the misbehaving device may inadvertently cause data traffic intended for the network node to be redirected to the misbehaving device.

SUMMARY

[0009] The following presents a simplified summary of one or more aspects in order to provide a basic understanding of such aspects. This summary is not an extensive overview of all contemplated aspects, and is intended to neither identify key or critical elements of all aspects nor delineate the scope of any or all aspects. Its sole purpose is to present some concepts of one or more aspects in a simplified form as a prelude to the more detailed description that is presented later.

[0010] In accordance with one or more aspects and corresponding disclosure thereof, various aspects are described in connection with authorization of devices to communicate directly with other devices utilizing the licensed spectrum. In accordance with some aspects, the authorization is based on prescribed user/service agreements. Configuration parameters that are employed to enable correct use of the spectrum can be vouched for by the spectrum provider authorization server and, thus, can be verified by peer devices. Such peer devices can be spectrum-authorized and are provided with authorized configuration parameters that can be utilized in the process of peer-to-peer/ad-hoc communication utilizing the spectrum.

[0011] An aspect relates to a method for validating ticket-based configuration parameters. The method includes associating a device with one or more validated information elements and transmitting an authorization ticket certified by a trusted party to the device. The ticket includes a subset of the one or more validated information elements, wherein the device uses the authorization ticket to establish a communication link with another device.

[0012] It should be noted that the process of validating the information elements is separate and distinct from the validation of authorization tickets. The trusted third party can obtain pre-validated information elements from another party or can validate the information elements itself through some other, separate process.

[0013] Another aspect relates to a wireless communications apparatus that includes a memory and a processor. The memory retains instructions related to associating a device with one or more validated information elements and transmitting an authorization ticket certified by a trusted party to the device. The ticket includes a subset of the one or more validated information elements, wherein the device uses the authorization ticket to establish a communication link with another device. The

processor is coupled to the memory and is configured to execute the instructions retained in the memory.

[0014] Yet another aspect relates to a wireless communications apparatus that provides ticket-based validation parameters. The apparatus includes means for associating a device with one or more validated information elements and means for transmitting an authorization ticket certified by a trusted party to the device. The ticket includes a subset of the one or more validated information elements. The device uses the authorization ticket to establish a communication link with another device.

[0015] Yet another aspect relates to a computer program product comprising a computer-readable medium. The computer-readable medium comprises a first set of codes for causing a computer to communicate with a device and a second set of codes for causing the computer to determine whether to create an authorization ticket for the device. The computer-readable medium also comprises a third set of codes for causing the computer to associate the device with one or more validated information elements and a fourth set of codes for causing the computer to communicate the authorization ticket to the device. The authorization ticket includes a subset of one or more validated information elements.

[0016] Yet another aspect relates to at least one processor configured to validate ticket-based configuration parameters. The processor includes a first module for consulting a database of authorized devices and associated parameters identified by a device identifier. The database contains information related to a configuration each device can use to communicate in a licensed spectrum. The processor also includes a second module for associating a device with one or more validated information elements and a third module for transmitting an authorization ticket certified by a trusted party to the device. The ticket includes a subset of the one or more validated information elements and the information related to the configuration the device can use to communicate, wherein the device uses the authorization ticket to establish a communication link with another device.

[0017] Still another aspect relates to a method for validation of ticket-based configuration parameters. The method includes obtaining an authorization ticket that includes one or more validated information elements associated with a device and validating the authorization ticket. The method also includes utilizing the authorization

ticket to establish a validated communication with the device and using a subset of the one or more validated information elements to perform a configuration operation.

[0018] A further aspect relates to a wireless communications apparatus comprising a memory and a processor. The processor is coupled to the memory and is configured to execute the instructions retained in the memory. The memory retains instructions related to obtaining an authorization ticket that includes one or more validated information elements associated with a device and validating the authorization ticket. The memory also retains instructions related to utilizing the authorization ticket to establish a validated communication with the device and using a subset of the one or more validated information elements to perform a configuration operation.

[0019] Still another aspect relates to a wireless communications apparatus that validates ticket-based configuration parameters. The apparatus includes means for acquiring an authorization ticket that includes one or more validated information elements associated with a device and means for validating the authorization ticket. The apparatus also includes a means for establishing a validated communication with the device based in part on the authorization ticket and a means for performing a configuration operation with a subset of the one or more validated information elements.

[0020] A further aspect relates to computer program product that includes a computer-readable medium. The computer-readable medium includes a first set of codes for causing a computer to obtain an authorization ticket that includes one or more validated information elements associated with a device and a second set of codes for causing the computer to validate the authorization ticket. The computer-readable medium also includes a third set of codes for causing the computer to utilize the authorization ticket to establish a validated communication with the device and a fourth set of codes for causing the computer to use a subset of the one or more validated information elements to perform a configuration operation.

[0021] Yet another aspect relates to at least one processor configured to provide spectrum authorization and access control. The processor includes a first module for acquiring an authorization ticket that includes one or more validated information elements associated with a device and a second module for validating the authorization ticket. The processor also includes a third module for employing the authorization ticket to establish a validated communication with the device and a fourth module for

utilizing a subset of the one or more validated information elements to perform a configuration operation.

[0022] To the accomplishment of the foregoing and related ends, the one or more aspects comprise the features hereinafter fully described and particularly pointed out in the claims. The following description and the annexed drawings set forth in detail certain illustrative features of the one or more aspects. These features are indicative, however, of but a few of the various ways in which the principles of the various aspects may be employed. Other advantages and novel features will become apparent from the following detailed description when considered in conjunction with the drawings and the disclosed aspects are intended to include all such aspects and their equivalents.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] Fig. 1 illustrates a wireless communication system in accordance with various aspects.

[0024] Fig. 2 illustrates a system for spectrum use authorization.

[0025] Fig. 3 illustrates a flow diagram of the operation of a device obtaining authorization from an authorization server.

[0026] Fig. 4 illustrates an example authorization ticket that can be utilized with the disclosed aspects.

[0027] Fig. 5 illustrates a flow diagram of an operation of two devices establishing a validated communication link by first validating spectrum use authorization and/or associated configuration parameters in accordance with the various aspects disclosed herein.

[0028] Fig. 6 illustrates a system for ticket-based spectrum authorization and access control in accordance with one or more aspects.

[0029] Fig. 7 illustrates a system for spectrum authorization and access control.

[0030] Fig. 8 illustrates a system for validation of ticket-based configuration parameters.

[0031] Fig. 9 illustrates another system for validation of ticket-based configuration parameters.

[0032] Fig. 10 illustrates a method for spectrum authorization and access control.

[0033] Fig. 11 illustrates a method for spectrum authorization and access control.

[0034] Fig. 12 illustrates a method for validating ticket-based configuration parameters.

[0035] Fig. 13 illustrates a method for validation of ticket-based configuration parameters.

[0036] Fig. 14 illustrates a system that facilitates ticket based authorization and validation in accordance with the disclosed aspects.

[0037] Fig. 15 illustrates an example system that facilitates spectrum authorization and access control in an ad hoc (peer-to-peer) environment.

[0038] Fig. 16 illustrates an example system that provides spectrum authorization.

[0039] Fig. 17 illustrates an example system that validates ticket-based configuration parameters in a communication environment.

[0040] Fig. 18 illustrates an example system that validates ticket-based configuration parameters.

DETAILED DESCRIPTION

[0041] Various aspects are now described with reference to the drawings. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of one or more aspects. It may be evident, however, that such aspect(s) may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to facilitate describing these aspects.

[0042] As used in this application, the terms "component", "module", "system", and the like are intended to refer to a computer-related entity, either hardware, firmware, a combination of hardware and software, software, or software in execution. For example, a component may be, but is not limited to being, a process running on a processor, a processor, an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a computing device and the computing device can be a component. One or more components can reside within a process and/or thread of execution and a component may be localized on one computer and/or distributed between two or more computers. In addition, these

components can execute from various computer readable media having various data structures stored thereon. The components may communicate by way of local and/or remote processes such as in accordance with a signal having one or more data packets (*e.g.*, data from one component interacting with another component in a local system, distributed system, and/or across a network such as the Internet with other systems by way of the signal).

[0043] Furthermore, various aspects are described herein in connection with a device. A device can also be called, and may contain some or all of the functionality of a system, subscriber unit, subscriber station, mobile station, mobile, wireless terminal, device, mobile device, remote station, remote terminal, access terminal, user terminal, terminal, wireless communication device, wireless communication apparatus, user agent, user device, or user equipment (UE). A mobile device can be a cellular telephone, a cordless telephone, a Session Initiation Protocol (SIP) phone, a smart phone, a wireless local loop (WLL) station, a personal digital assistant (PDA), a laptop, a handheld communication device, a handheld computing device, a satellite radio, a wireless modem card and/or another processing device for communicating over a wireless system. Moreover, various aspects are described herein in connection with a base station. A base station may be utilized for communicating with wireless terminal(s) and can also be called, and may contain some or all of the functionality of, an access point, Node B, or some other network entity.

[0044] Various aspects or features will be presented in terms of systems that may include a number of devices, components, modules, and the like. It is to be understood and appreciated that the various systems may include additional devices, components, modules, *etc.* and/or may not include all of the devices, components, modules *etc.* discussed in connection with the figures. A combination of these approaches may also be used.

[0045] Referring now to **Fig. 1**, illustrated is a wireless communication system 100 in accordance with various aspects. System 100 comprises a base station 102 that can include multiple antenna groups. For example, one antenna group can include antennas 104 and 106, another group can comprise antennas 108 and 110, and an additional group can include antennas 112 and 114. Two antennas are illustrated for each antenna group; however, more or fewer antennas can be utilized for each group. Base station 102 can additionally include a transmitter chain and a receiver chain, each

of which can in turn comprise a plurality of components associated with signal transmission and reception (*e.g.,* processors, modulators, multiplexers, demodulators, demultiplexers, antennas, *etc.*), as will be appreciated by one skilled in the art. Additionally, the base station 102 can be a home base station, a Femto base station, and/or the like.

[0046] Base station 102 can communicate with one or more devices such as device 116; however, it is to be appreciated that base station 102 can communicate with substantially any number of devices similar to device 116. As depicted, device 116 is in communication with antennas 104 and 106, where antennas 104 and 106 transmit information to device 116 over a forward link 118 and receive information from device 116 over a reverse link 120.

[0047] In a frequency division duplex (FDD) system, forward link 118 can utilize a different frequency band than that used by reverse link 120, for example. Further, in a time division duplex (TDD) system, forward link 118 and reverse link 120 can utilize a common frequency band.

[0048] In addition, devices 122 and 124 can be communicating with one another, such as in a peer-to-peer configuration. Moreover, device 122 is in communication with device 124 using links 126 and 128. In a peer-to-peer ad hoc network, devices within range of each other, such as devices 122 and 124, communicate directly with each other without a base station 102 and/or a wired infrastructure to relay their communication. Additionally, peer devices or nodes can relay traffic. The devices within the network communicating in a peer-to-peer manner can function similar to base stations and relay traffic or communications to other devices, functioning similar to base stations, until the traffic reaches its ultimate destination. The devices can also transmit control channels, which carry information that can be utilized to manage the data transmission between peer devices.

[0049] A communication network can include any number of devices or nodes that are in wireless communication. Each device or node can be within range of one or more other devices or nodes and can communicate with the other devices/nodes or through utilization of the other devices/nodes, such as in a multi-hop topography (*e.g.,* communications can hop from node to node until reaching a final destination). For example, a sender device may wish to communicate with a receiver device. To enable packet transfer between sender device and receiver device, one or more intermediate

devices can be utilized. It should be understood that any device can be a sender device and/or a receiver device and can perform functions of either sending and/or receiving information at substantially the same time (*e.g.,* can broadcast or communicate information at about the same time as receiving information and/or at a different time).

[0050] System 100 can be configured to enable usage of a spectrum for data communication by authorized devices, wherein devices that are not authorized (*e.g.,* traditional or common devices) cannot use the spectrum. Authorization tickets can be distributed by a trusted third party after validation of a device's credentials and the services to which the device is entitled. Further, system 100 can mandate the exchange and verification of authorization tickets by devices as a condition for configuring a wireless link utilizing the spectrum.

[0051] **Fig. 2** illustrates a system 200 for spectrum use authorization. System 200 can be configured to enable communications authorized (or vouched for) by a spectrum provider (or a trusted third party) to occur between devices (*e.g.,* in a peer-to-peer manner) or between devices and base stations.

[0052] System 200 includes an authorization server 202 and a configuration parameters database 204. The authorization server 202 can be co-located or communicatively coupled to the configuration parameters database 204. Also included in system 200 are devices, labeled device$_1$ 206 and device$_N$ 208, where N is an integer. Devices 206, 208 can be mobile devices and/or base stations that operate similar to mobile devices in accordance with the disclosed aspects (*e.g.,* the fact that the base stations are typically connected to other networks or infrastructure is not relevant to the disclosed aspects). Devices 206, 208 can communicate with each other (illustrated by bidirectional communication link 210), and with other devices wirelessly. Further, devices 206, 208 can communicate with authorization server 202 wirelessly or through wired links (illustrated by bidirectional communication links 212 and 214). If the communication between a device 206, 208 and the authorization server 202 is wireless, the communication may or may not be through a licensed spectrum, such as the licensed spectrum that is used by devices 206, 208 to communicate with each other. In accordance with some aspects, the link between devices (link 210) and the links between one or more devices 206, 208 and the authorization server 202 (links 212 or 214) can be the same link or a similar link.

[0053] Authorization server 202 can selectively distribute authorization for use of a spectrum, such as a licensed spectrum, to one or more devices 206, 208. The authorization can be distributed in the form of an authorization ticket, illustrated as authorization ticket_1 216 and authorization ticket_M 218, where M is an integer. The authorization ticket 216, 218 can include various information such as a device identifier, a validity period, a cryptographic signature of the authorizing device (*e.g.,* authorization server 202), as well as other information. Further information relating to the authorization ticket will be provided below.

[0054] The authorization tickets 216, 218 can be utilized by the devices 206, 208 to enable communication among the devices 206, 208. In accordance with some aspects, the authorization tickets 216, 218 can be utilized to authorize a certain use (*e.g.,* to authorize services) of the spectrum. In accordance with some aspects, the authorization tickets 216, 218 can be distributed to the one or more devices 206, 208 using a network layer protocol. It should be understood that a device to which authorization to the (licensed) spectrum is not given does not receive an authorization ticket.

[0055] To distribute the authorization tickets, authorization server 202 can periodically (*e.g.,* once a month, another predetermined interval) communicate with the one or more devices 206, 208 and provide the appropriate authorization ticket to each device individually. For example, authorization server 202 can transmit a new authorization ticket having a different validity range than an authorization ticket that was previously transmitted to the device. Each device 206, 208 receives an authorization ticket that is different from an authorization ticket provided to another device. For example, authorization server 202 transmits authorization ticket_1 216 to device_1 206 and authorization ticket_M 218 to device_N 208. Each device 206, 208 can retain its authorization ticket, such as in a storage media.

[0056] The devices 206, 208 exchange the authorization tickets to establish a validated communication link 210 between each other. Thus, device_1 206 sends authorization ticket_1 216 to device_N 208 and device_N 208 sends authorization ticket_M 218 to device_1 206. Validation of the authorization tickets allows the devices (*e.g.,* two mobile devices, a mobile device and an access point, and so forth) to communicate in a peer-to-peer manner in accordance with the disclosed aspects. If a device is not able to

validate the authorization ticket of the device to which it desires to communicate, a validated communication link is not established between the devices.

[0057] **Fig. 3** illustrates a flow diagram 300 of the operation of a device obtaining authorization from an authorization server. The authorization server 202 can be a trusted party that issues authorization tickets to devices, such as $Device_1$ 206. It should be appreciated that authorization server 202 can issue authorization tickets to a multitude of devices at substantially the same time, or at different times. However, only one device is illustrated for purposes of simplicity.

[0058] To initiate issuance of an authorization ticket, the device 206 sends an Authorization Request Message 302 that contains at least a unique identifier of the device (*e.g.,* Device_ID_1). In accordance with some aspects, the Authorization Request Message 302 can include other credential information, such as a public key.

[0059] The device 206 can be triggered to send the Authorization Request Message 302 based on detection of an upcoming expiration of a previously obtained authorization ticket (*e.g.,* the authorization ticket the device is currently using to communicate with other devices). In accordance with some aspects, sending the Authorization Request Message 302 can be triggered by an order for user applications to enable a wireless link while there is no valid authorization ticket retained in the device (*e.g.*, in a storage medium).

[0060] Additionally or alternatively, the device 206 can be triggered to send the Authorization Request Message 302 based on a request received from the authorization server 202. The authorization server 202 can transmit the request for administrative reasons and/or based on an indication that an amount or quota of data that was authorized to be sent/received by the device under the previous authorization ticket has been (or will be) exceeded. In this alternative aspect, a message (not shown) is received from the authorization server 202 prior the transmission of the Authorization Request Message 302.

[0061] At substantially the same time as receiving the Authorization Request Message 302, the authentication server 202 verifies the identity of the device 206 and the services to which the device 206 is entitled (*e.g.,* the services that have been purchased, services allowed under a current plan, services allowed for no cost during a promotion period, and so forth). This is illustrated by the double bidirectional arrows at 304 (Authentication Mechanism). This verification process can be referred to as

"authentication", "authorization", "accounting protocol", and/or "authentication protocol". Examples of such protocols include Transport Level Security (TLS), Internet Key Exchanges (IKE), and others.

[0062] In accordance with some aspects, device 206 sends credential information in response to a channel message sent by authorization server 202 as part of the message exchange 304. According to other aspects, both the device 206 and the authorization server 202 exchange respective credential information in order to perform a mutual authentication procedure and typically secure the communication channel between the device 206 and authorization server 202.

[0063] If the identity of the device 206 is verified, the authentication server 202 assigns/generates configuration parameters and includes this information in an authorization ticket created by the authentication server 202. Additionally or alternatively, authentication server 202 can assign/generate the configuration parameters in conjunction with one or more other databases or servers.

[0064] In accordance with some aspects, the newly created authorization ticket is substantially the same as a previous authorization ticket provided to the device 206. However, the newly created authorization ticket can have a different validity period (start time/end time) and a different cryptographic signature. In accordance with some aspects, the newly created authorization ticket can include authorization for services that are the same or different from the services authorized by the previous authorization ticket (*e.g.,* more services, less services, different services). Further information relating to the authorization ticket will be described in further detail with reference to Fig. 4.

[0065] The newly created authorization ticket is sent to the device 206 in an Authorization Response Message 306. According to some aspects, the authorization ticket might be encrypted with the intent that the ticket can only be decrypted by the device for which it is intended (*e.g.,* device 206). The device 206 can retain the authorization ticket in a storage medium for later use to establish a validated communication link with other devices.

[0066] **Fig. 4** illustrates an example authorization ticket 400 that can be utilized with the disclosed aspects. It should be understood that the illustrated and described authorization ticket 400 is provided for ease of understanding this detailed description and other authorization tickets can be utilized.

[0067] Included in authorization ticket 400 are a device identifier 402, a validity period 404, and a cryptographic signature 406 of the authorizing server, covering the entire ticket 400 data. The validity period 404 includes a start time (*e.g.,* not before: <date/time>) and an end time (*e.g.,* not after: <date/time>). A validity period 404 can create a level of security because, if an authorization ticket is fraudulently obtained by a misbehaving device, upon expiration, that authorization ticket will no longer be usable by the misbehaving device.

[0068] In accordance with an optional aspect, the authorization ticket 400 can contain information that can be utilized to authenticate the ticket holder (*e.g.,* device). This information, represented as optional by the dashed line at 408, can be in the form of a digital certificate, a public key, a hash of a public key belonging to the device as indicated by the device identifier 402, as well as other authentication means.

[0069] Additionally or alternatively, the authorization ticket 400 can include an optional (denoted by the dashed line) list of (or a representation of) the types services 410 that the device, identified by device identifier 402, is permitted to consume using the spectrum in a peer-to-peer or a group manner (*e.g.,* voice or video calls, data exchange with a maximum or minimum rate, receipt of special broadcast information, and so forth). According to some aspects, the information 410 on allowed services is taken into account by other devices that are validating the ticket 400 such that the other device(s) can decide whether and how to enable a validated communication link. If the valid communication link is enabled, the other device(s) can configure the link to carry only the type of data and/or data rate as specified in a list of the type of services allowed.

[0070] The authorization ticket 400 may also optionally contain (as noted by the dashed line) other configuration or enabling information 412. This other information 412 can include a piece of data given out to all authorized devices and utilized in an ad-hoc network to configure the physical or media access control channels, so that only authorized devices can communicate using these channels. In accordance with some aspects, the other information 412 includes configuration information and/or an assigned parameters list, which can be utilized by other devices that are validating the authorization ticket in order for the other devices to determine how to correctly configure the link.

[0071] **Fig. 5** illustrates a flow diagram 500 of an operation of two devices establishing a validated communication link by first validating spectrum use authorization and/or associated configuration parameters in accordance with the various aspects disclosed herein. When a first device ($Device_1$) 206 desires to communicate with one or more other devices ($Device_N$) 208, using the spectrum, the first device 206 transmits a Connection Request Message 502. The Connection Request Message 502 includes an identifier of the first device 206 (*e.g.,* "ID-Device-1"). In accordance with some aspects, the Connection Request Message 502 includes an authorization ticket that identifies (and that belongs) to the first device 206.

[0072] The second device 208 can respond to the Connection Request Message 502 with a Connection Response Message 504 that contains an identifier of the second device 206 (*e.g.,* "ID-Device-*N*"). In accordance with some aspects, the Connection Response Message 504 can be transmitted after second device 208 verifies the contents of the authorization ticket received from first device 206. The Connection Response Message 504 can include an authorization ticket that identifies (and that belongs to) the second device 208. At substantially the same time as receiving the Connection Response Message 504, first device 206 can verify the contents of the authorization ticket received from second device 208.

[0073] Either or both the Connection Request Message 502 and the Connection Response Message 504 can contain the public keys(s) associated with the device sending the message (*e.g.,* "public-key-1", "public-key-*N*"). In accordance with some aspects, either or both messages 502, 504 include a complete digital certificate.

[0074] In an optional aspect as denoted by dashed line 506, one or more other messages can be exchanged. These other messages 506 can be sent with the purpose of achieving mutual identity authentication. For example, first device 206 can authenticate the identity of second device 208 (*e.g.* verify identity "ID-Device-*N*") and the second device 208 can authenticate the identity of first device 206 (*e.g.,* verify identity "ID-Device-1").

[0075] A purpose of messages 502, 504, and optionally 506, is to achieve mutual identity authentication. The mutual identity authentication is different from the authorization verification process. In accordance with some aspects, both the mutual identity authentication and the authorization verification processes can be performed at substantially the same time.

[0076] According to various aspects, identity authentication can be achieved by employing digital certificates. For example, two devices 206, 208 can engage in a protocol whereby each device transmits their certificate and other information (*e.g.,* a random number or nonce). This exchange can assist to verify that the other device is indeed in possession of the private key associated with the presented certificate.

[0077] In accordance with some aspects, the identity authentication can also result in establishing a shared secret key that can be utilized to secure the communication channel between devices 206 and 208.

[0078] According to other aspects, the digital certificate utilized for identity authentication and establishment of communication channel security can be the same as the spectrum authorization ticket. In this case, the identity authentication task and the authorization tasks are combined.

[0079] An authorization exchange takes place wherein the first device 206 sends an Authorization Request Message 508 to the second device 208. The Authorization Request Message 508 can include an authorization ticket of the first device 206. The second device 208 can respond with an Authorization Response Message 510 that can contain an authorization ticket of the second device 208.

[0080] At substantially the same time as receiving the Authorization Request Message 508, the second device 208 can verify the received authorization ticket (included in the message) of the first device 206. In a similar manner, at substantially the same time as receiving an Authorization Response Message 510, the first device 206 can verify the authorization ticket (included in the message) of the second device 208. Verification of the respective authorization tickets include confirming that the identifier in the ticket is the same identifier as the identifier that was validated during the mutual identity authentication, as discussed above.

[0081] It should be noted that, in accordance with some aspects, only verifying the authorization ticket might not be enough to achieve a proper amount of security. Therefore, the verification process can also include device or user identity authentication. According to this aspect, "authorization ticket verification" refers to the verification of the server-generated ticket (*e.g.,* authorization ticket) and that the ticket belongs to the device sending the ticket, as identified by the identifier included in the ticket. Additionally or alternatively, the authorization ticket either has the form of a digital certificate or also includes a device or user digital certificate. Thus, in

accordance with this aspect, each device needs to prove that it is the rightful owner of the presented authorization ticket. In accordance with some aspects, ownership of a digital certificate can be verified by showing a verified entity proof of possession of a private key associated with a public key that is present in the certificate.

[0082] In an optional aspect, as represented by dashed line 512, another security and/or configuration protocol may be administered between devices 206 and 208 for the purpose of secure key derivation and possibly other configurations.

[0083] After completion of the mutual verification of identities and authorization tickets, a link is configured utilizing the information/assigned parameters included in the exchanged authorization tickets. After configuration of the valid link, user data can be exchanged, at 514, between the devices 206 and 208 over the validated communication link.

[0084] It should be noted that the flow chart illustrated and described with reference to Fig. 5 is for illustration purposes only. For example, the mutual verification of identities and authorization tickets can be performed at times other than upon receipt of a connection message. Further, tasks such as identity verification and authorization verification can be combined. Additionally, entities can be exchanged and verified at a later time as part of the authorization ticket exchange and associated security protocols. Additionally or alternatively, messages sent by the first device 206 can be combined (*e.g.,* messages 502 and 508; messages 502, 506, 508, and 512) in one or several messages. In a similar manner, messages from the second device 208 can be combined (*e.g.,* messages 504 and 510; messages 504, 506, 510 and 512) in one or several messages.

[0085] In accordance with some aspects, authorization tickets can be obtained by a first device 206 through means other than directly from the second device 208. For example, the second device 208 can transmit its (unique) identifier and the first device 206 utilizes the identifier to retrieve and verify the second device's authorization ticket, which can be obtained from a server or local database.

[0086] According to various aspects, both devices 206, 208 verify the other device's identity and authorization ticket prior to allowing user data or other protocol data to flow, at 514, on the shared wireless link using the spectrum. It should also be understood that a similar process could be undertaken by more than two devices (*e.g.,* when group wireless communication is employed using broadcast/multicast

mechanisms). In multi-device scenarios, each device should successfully validate the authorization tickets granted to the other devices in the communication group prior to activating the wireless link or links to carry other data.

[0087] According to some optional aspects, other enforcement schemes can be utilized at substantially the same time as the spectrum use authorization validation described herein. For example, wireless sensor points can be placed over a geographical area. These sensor points can listen for unauthorized wireless data exchange. In another example, legitimate nodes can actively listen and report communication that was not preceded by the exchange of valid authorization tickets if the system requires that tickets to be explicitly exchanged.

[0088] In accordance with another aspect, first device 206 obtains an authorization ticket (*e.g.,* from an authentication server) authorizing spectrum-use services of type "A" only (*e.g.,* voice calls only). When establishing a communication between first device 206 and another device (*e.g.,* second device 208), each device transmits its authorization ticket to the other device. If the second device 208 is entitled to services of type "A", the link is enabled for exchanging data of type "A" only. If at a later time, first device 206 desires to exchange data of type "B" (*e.g.,* video) with second device 208, second device 208 does not cooperate because second device 208 is configured to not allow such data (*e.g.,* type "B") to be sent and/or received.

[0089] With reference now to **Fig. 6**, illustrated is a system 600 for ticket-based spectrum authorization and access control in accordance with one or more aspects. System 600 can be configured to enable a spectrum licensee/owner to extract revenue from devices communicating utilizing the (radio frequency) spectrum in an ad-hoc or peer-to-peer manner, without the need for controlled infrastructure. System 600 can enable the use of the spectrum for data communication by authorized devices though the distribution of authorization tickets and the exchange and verification of these authorization tickets between the devices for enablement of a validated wireless link that carries user or control data communications. Included in system 600 is a wireless communications apparatus 602 that can be in communication with one or more devices 604 and one or more trusted parties 606, which can be a node.

[0090] Wireless communications apparatus 600 includes an authorization ticket requestor 608 that obtains an authorization ticket issued for wireless communications apparatus 602. The authorization ticket for the wireless communications apparatus 602

is issued by a trusted third party 606. In accordance with some aspects, the trusted parties 606 can be authorization server(s) that issue authorization tickets.

[0091] In accordance with some aspects, communication with the trusted parties 606 (or authorization server(s)) is conducted through an interface, which can be a cellular wireless interface, a wired interface such as a Digital Subscriber Line (DSL), cable, and so forth.

[0092] Also included in wireless communications apparatus 600 is an associated device authorization ticket acquirer 610 that is configured to request or receive an authorization ticket from an associated device(s) 604 (*e.g.,* a device to which communication is to be established). The authorization ticket is issued to the one or more associated devices 604 from the trusted third party that issued the authorization ticket for wireless communications apparatus 602 or from another trusted party. The authorization ticket of the associated device(s) 604 can include a validity time or cryptographic signature of the trusted party that issued the ticket.

[0093] According to some aspects, the authorization ticket of wireless communications apparatus 602 and/or the authorization ticket(s) of the associated device(s) 604 are embodied as a traditional digital certificate (*e.g.,* X.509 standard). For example, a traditional digital certificate can include extensions to indicate authorization for spectrum use and/or can convey other information pertaining to establishing validated communication links.

[0094] A verification module 612 is configured to establish a valid communication session between the wireless communications apparatus 602 and one or more associated devices 604. The verification module 612 can validate the authorization ticket for the associated device (s). According to some aspects, the validated communication session can be secured based on information contained in the authorization ticket of wireless communication apparatus 602 and the authorization ticket(s) of the associated device(s) 604. A secured communication session refers to a communication session that has encryption/decryption and integrity protection.

[0095] In accordance with some aspects, the authorization ticket issued for wireless communications apparatus 602 is transmitted to the associated device (s) 604 in order for the associated device(s) to verify the identity of wireless communications apparatus 602 and to establish a validated communication session. Data between wireless communications apparatus 602 and the one or more devices 604 is not enabled

to carry data until the authorization ticket exchange has been successfully conducted and the link has been validated.

[0096] In accordance with some aspects, a cellular interface can be utilized to enable communication between wireless communications apparatus 602, the device(s) 604, and/or the trusted parties 606. Although the cellular interface can be mostly for communication with other device(s) 604, the interface can be utilized for communication with access points (or base stations). For example, a cellular interface can carry data wirelessly from wireless communications apparatus 602 to an access point and from there onto one or more trusted third party 606. It should be noted, however, that the presence or involvement of access points is not necessary. Data can also be relayed through one or more other device, one of which is eventually connected to the network where a trusted third party 606 resides.

[0097] According to some aspects, the communication between wireless communications apparatus 602 and one or more trusted third party 606 is performed through a wireless interface. In accordance with this aspect, a direct point of communication may be another device or access point, which can in turn either relay the data to another entity that has a communication link with the trusted third party 606, or can send the data directly to the trusted third party 606. It should be noted that when implementing this aspect, communication through the interface using the licensed spectrum should not be enabled until after the authorization ticket is obtained (and verified). In one approach, the authorization protocol is run using this communications link, in the absence of another available interface, therefore, a means to bootstrap the authorization for spectrum use should be provided. It is understood that absent a valid authorization ticket, the communication through the interface is by configuration limited to only the protocol and data that pertains directly to the authorization process with the trusted party 606 (*e.g.,* obtaining an authorization ticket).

[0098] In another approach, the authorization protocol is run by a "helper" device or access point on behalf of the wireless communications apparatus 602 seeking authorization. Thus, the wireless communications apparatus 602 only uses the interface to locate another access point or device and requests that device to run the needed authentication/authorization protocol with the trusted party 606 on behalf of the wireless communications apparatus 602. This process can involve relaying of data between the wireless communications apparatus 602 and the helper counterpart.

[0099] System 600 can include memory 614 operatively coupled to wireless communications apparatus 602. Memory 614 can be external to wireless communications apparatus 602 or can reside within wireless communications apparatus 602. Memory 614 can store information related to obtaining a first authorization ticket associated with wireless communications apparatus 602. The first authorization ticket can be issued by a trusted third party. Memory 614 can also store information related to receiving from a second device a second authorization ticket for the second device. The second authorization ticket can be issued by the trusted third party or another trusted party. Further, memory 614 can retain instructions related to establishing a validated communication session with the second device or with a multitude of devices.

[00100] A processor 616 can be operatively connected to wireless communications apparatus 602 (and/or memory 614) to facilitate analysis of information related to spectrum authorization and access control in a peer-to-peer or ad hoc communication network. Processor 616 can be a processor dedicated to analyzing and/or generating information received by wireless communications apparatus 602, a processor that controls one or more components of system 600, and/or a processor that both analyzes and generates information received by wireless communications apparatus 602 and controls one or more components of system 600.

[00101] Memory 614 can store protocols associated with spectrum authorization, access control between wireless communications apparatus 602, device(s) 604, and/or trusted parties 606, such that system 600 can employ stored protocols and/or algorithms to achieve improved communications in a wireless network as described herein. Memory 614 can further retain an authorization ticket associated with wireless communications apparatus 602 and/or one or more devices 604.

[00102] Memory 614 can further retain instructions related to obtaining a first authorization ticket for a first device issued by a trusted third party, receiving from a second device a second authorization ticket for the second device, the second authorization ticket is issued by the trusted third party or another trusted party, and establishing a validated communication session with the second device. The processor 616 is configured to execute the instructions retained in the memory.

[00103] It should be appreciated that the data store (*e.g.,* memories) components described herein can be either volatile memory or nonvolatile memory, or can include both volatile and nonvolatile memory. By way of example and not limitation,

nonvolatile memory can include read only memory (ROM), programmable ROM (PROM), electrically programmable ROM (EPROM), electrically erasable ROM (EEPROM), or flash memory. Volatile memory can include random access memory (RAM), which acts as external cache memory. By way of example and not limitation, RAM is available in many forms such as synchronous RAM (DRAM), dynamic RAM (DRAM), synchronous DRAM (SDRAM), double data rate SDRAM (DDR SDRAM), enhanced SDRAM (ESDRAM), Synchlink DRAM (SLDRAM), and direct Rambus RAM (DRRAM). Memory 614 of the disclosed aspects are intended to comprise, without being limited to, these and other suitable types of memory.

[00104] **Fig. 7** illustrates a system for spectrum authorization and access control 700. System 700 is similar to system 600 of Fig. 6 and includes a device 702 that communicates with other devices 704 and with one or more trusted parties, illustrated as wireless communication apparatus 706.

[00105] A trusted party 706 can include a receiver 708 that is configured to receive a request from a first device, such as device 702, for system access. Receiver 708 can also receive requests from one or more of the other devices 704 at substantially the same time as receiving a request from first device 702, at a different time, or combinations thereof.

[00106] Based on the request, an authenticator 710 can be configured to obtain authentication of the first device 702 (or another device that transmitted the request). In accordance with some aspects, the first device authentication is obtained from an external source, such as from a network device over a secure communication link and/or from a home server. For example, the external source can be a server that has a business relationship with the first device (*e.g.,* user in possession of the device) and the server can verify the subscription (*e.g.,* the services for which the user has subscribed).

[00107] Based in part on the authentication of the first device 702, an access authorizer 712 can determine the system access that can be authorized for the first device 702 (or another device 704). According to some aspects, access authorizer 712 can consult a configuration parameters database that contains a listing of a plurality of devices that are authorized to access the system to determine the access to which the first device is entitled. The configuration parameters database can also contain one or more configuration parameters (*e.g.,* a set of configuration parameters) associated with each device. If first device is included in the listing, the first device is authorized to

access the system. However, if first device is not included in the listing, the first device is not authorized to access the system. The configuration parameters database can be dynamically updated, such as when there is a change to the database and/or based on other criteria.

[00108] In accordance with some aspects, authenticator 710 and/or or access authorizer 712 can review credentials associated with the first device 702 (or another device 704) to make respective determinations. The credentials can be at least one of shared secret keys, public keys, authorization information, a list of services, billing information, or combinations thereof.

[00109] Authorization ticket generator 714 can create an authorization ticket for the first device 702 (and/or the other devices 704) based on the authorized system access as determined by access authorizer 712. A part of the authorization ticket creation can include the generation of a cryptographic signature on which the validity of the authorization ticket relies. The authorization ticket can include an identity of the first device, a validity range during which the authorization ticket is valid, a cryptographic signature, and/or other parameters.

[00110] System 700 can include a memory 716 operative connected to (or included within) wireless communications apparatus 706. Memory 716 can store instructions related to receiving a request from at least a first device for system access, performing authentication of the at least a first device, determining system access that can be authorized for the first device, and generating an authorization ticket for the at least a first device based in part on the authorized system access. A processor 718 can be coupled to the memory 716 and can be configured to execute the instructions retained in the memory 716.

[00111] With reference now to **Fig. 8**, illustrated is a system 800 for validation of ticket-based configuration parameters. System 800 can be configured to enable authorized devices to communicate over a licensed spectrum through the utilization of authorization tickets. A device that desires to communicate with another device can verify link configuration parameters claimed by the other device have been authorized by a mutually trusted third party.

[00112] Included in system 800 is a wireless communications apparatus 802 that can be, for example a trusted third party, such as an authorization server. Wireless

communications apparatus 802 is configured to communicate with one or more devices, labeled Device$_1$ 804 through Device$_P$ 806, where P is an integer.

[00113] Included in wireless communication apparatus 802 is device identifier 808 that can selectively recognize each device 804, 806 based, in part, on a request for system access. For example, each device 804, 806 can be identified by a unique identifier, such as a hardware address. Further, device identifier 808 can include other authentication and/or authorization information associated with each device 804, 806. For example, credentials such as shared secret keys, public keys, authorization information, a list of services each device is entitled to, associated billing/charging information, and so forth can be retained by (or accessible by) device identifier 808.

[00114] In accordance with some aspects, device identifier 808 includes a configuration parameters database that can contain a database of devices that are authorized for using the spectrum. The database can also contain configuration information and/or assigned parameters for each device. In accordance with some aspects, a subset of the parameters can be generated at the time a request for authorization is received from a device. Other parameters, such as IP addresses, can be assigned from a pool of available addresses and/or obtained from another server. In accordance with some aspects, configuration information can be stored as dictated by service agreements and the like.

[00115] If the device identifier 808 does not have (or cannot obtain) all the necessary information for one or more devices 804, 806, the information can be obtained from another server or network device that holds, or has access to, the needed information in its entirety or in part. Obtaining the information from another server or network device can be conducted in a secure manner. In this situation, wireless communications apparatus 802 can utilize a communication interface to communicate with another server that holds authentication/authorization information for all or some devices 804, 806. In accordance with some aspects, information associated with some or all devices 804, 806 can reside at multiple network nodes.

[00116] The purpose of consulting a database is to check the identity of the device seeking authorization and to determine the services the device is entitled to according to a user service agreement or the like. Consulting the database is a portion of the process that wireless communication apparatus 802 conducts for each device 804, 806 seeking system access.

[00117] An authorization ticket distributor 810 selectively distributes authorization tickets to devices 804, 806. The distribution of authorization tickets can be a result of validating a device's credentials and the services the device is entitled to have access to and to utilize. Further, the authorization tickets are exchanged between devices and verified as a condition to bringing up or enabling a wireless link using the spectrum to carry user or control data communication. In such a manner, only authorized devices are enabled to use the spectrum for data communication in accordance with the aspects presented herein. According to some aspects, the authorization ticket is implements as a traditional digital certificate, such as a X.509 certificate, that can include an IP address.

[00118] Further, a memory 812 can be operatively coupled to wireless communications apparatus 802. Memory 812 can be external to wireless communications apparatus 802 or can reside within wireless communications apparatus 802. Memory 812 can store information related to associating a device with one or more validated information elements and transmitting an authorization ticket, certified by a trusted party to the device. The ticket can include a subset of the one or more validated information elements.

[00119] Retaining the authentication ticket in memory can mitigate the need to obtain the authentication ticket when a validated communication session is to be established. Thus, if the authentication server and/or source of the authentication ticket is not available (*e.g.,* limited connectivity), the authentication ticket retained in memory can be utilized. In accordance with some aspects, an updated authentication ticket is obtained when connectivity is restored.

[00120] Information elements can be expressions, addresses, a phone number, and/or other information that is to be presented to a user (*e.g.,* visual information, audible information, and so forth). In accordance with some aspects, information elements can be configuration parameters and/or an IP address. Additionally or alternatively, information elements can be identifiers that are being broadcast and or advertised. Further, information elements can be a name, an identity, a location, user information (*e.g.,* an emotion the user wants to express), a trademark, and any other data.

[00121] In accordance with some aspects, only a subset of available information elements is included in an authentication ticket. For example, if there are hundreds or

thousands of information elements that can be included in an authentication ticket, only a subset of those information elements might be included in the authentication ticket. The determination of which information elements to include can be a function of the source of the information elements (and authentication ticket) and/or the destination of the information elements (and authentication ticket).

[00122] The information elements can be validated in order to provide some reliability to the information elements. Validated information elements can mitigate the need to independently validate the information elements (*e.g.,* no need to access another device, another database, or any other source) since the information elements are pre-validated by the server.

[00123] A processor 814 can be operatively connected to wireless communications apparatus 802 (and/or memory 812) to facilitate analysis of information related to spectrum authorization and access control in an ad-hoc communication network. Processor 814 can be a processor dedicated to analyzing and/or generating information received by wireless communications apparatus 802, a processor that controls one or more components of system 800, and/or a processor that both analyzes and generates information received by wireless communications apparatus 802 and controls one or more components of system 800.

[00124] Memory 812 can store protocols associated with spectrum authorization, access control between wireless communications apparatus 802, device(s) 804, 806 and/or other trusted parties, such that system 800 can employ stored protocols and/or algorithms to achieve improved communications in a wireless network as described herein. In accordance with some aspects, memory retains instructions related to associating a device with one or more validated information elements and transmitting an authorization ticket, certified by wireless communications apparatus, to the device.

[00125] **Fig. 9** illustrates another system 900 for validation of ticket-based configuration parameters. System 900 is similar to the system of the above figure and includes an authentication server 902, a first device 904, and one or more other devices 906.

[00126] Device 904 can include a ticket acquirer 908 that obtains an authorization ticket. The authorization ticket can include one or more validated information elements associated with another device (*e.g.,* a device with which a validated communication session is to be established), this device will be referred to herein as second device 904.

At least one of the validated information elements is an Internet Protocol address. In accordance with some aspects, the authorization ticket includes an identifier of the second device 904, a validity range, and a signature of a trusted party that issued the authorization ticket to the second device 904. Also included in device 904 is a validation module 910 that validates the authorization ticket.

[00127] A communication establisher 912 utilizes the authorization ticket to establish a validated communication with the second device 904. The validated communication can be broadcast or multicast. In accordance with some aspects, the validated communication is with the second device 904 in a peer-to-peer or ad-hoc configuration. Additionally, the communication with the second device 904 can be over a secure communication link.

[00128] Device 904 also includes an operation execution module 914 that uses a subset of the one or more validated information elements to perform a configuration operation. The configuration operation can include configuring an interface and/or adding a route.

[00129] A memory 916 is operatively connected to device 904 and is configured to retain instructions related to obtaining an authorization ticket that includes one or more validated information elements associated with a second device. The memory also retains instructions related to validating the authorization ticket, utilizing the authorization ticket to establish a validated (and possibly secure) communication with the second device, and using a subset of the one or more validated information elements to perform a configuration operation. A processor 918 is coupled to the memory 916 and is configured to execute the instructions retained in the memory 916.

[00130] In view of the exemplary systems shown and described, methodologies that may be implemented in accordance with the disclosed subject matter, will be better appreciated with reference to the flow charts provided herein. While, for purposes of simplicity of explanation, the methodologies may be shown and described as a series of blocks, it is to be understood and appreciated that the claimed subject matter is not limited by the number or order of blocks, as some blocks may occur in different orders and/or at substantially the same time with other blocks from what is depicted and described herein. Moreover, not all illustrated blocks may be required to implement the methodologies described herein. It is to be appreciated that the functionality associated with the blocks may be implemented by software, hardware, a combination thereof or

any other suitable means (*e.g.* device, system, process, component). Additionally, it should be further appreciated that the methodologies disclosed throughout this specification are capable of being stored on an article of manufacture to facilitate transporting and transferring such methodologies to various devices. Those skilled in the art will understand and appreciate that a methodology could alternatively be represented as a series of interrelated states or events, such as in a state diagram.

[00131] **Fig. 10** illustrates a method 1000 for spectrum authorization and access control. Method 1000 can enable utilization of a spectrum by authorized devices operating in an ad-hoc or peer-to-peer fashion, without the need for a controlled infrastructure.

[00132] Method 1000 starts, at 1002, when a first authorization ticket is obtained from a trusted third party. The trusted third party can be, for example, an authorization server. The authorization ticket can include an identifier of a device and a signature of the trusted third party. In accordance with some aspects, the first authorization ticket is transmitted to a second device.

[00133] A second authorization ticket is received from an associated device, at 1004. The second authorization ticket can be issued by the trusted third party that issued the first authorization ticket or the second authorization ticket can be issued by another trusted party. The second authorization ticket can include a validity time or a cryptographic signature of the trusted party that issued the second authorization ticket (*e.g.,* the trusted third party or the another trusted party). In accordance with some aspects, the first authorization ticket comprises services allowed to be accessed by the first device and the second authorization ticket comprises services allowed to be accessed by the second device.

[00134] A valid communication session with the associated device is established, at 1006. The validated communication session can be configured to carry data of a type and manner specified in a list of allowed services included in the first authorization ticket and the second authorization ticket.

[00135] In accordance with some aspects, establishing the valid communication session can include validating the second authorization ticket. A failure to validate the second authorization ticket for the second device can result in tearing down a communication link between the first device and the second device. Validating the second authorization ticket can include verifying a validity time and a cryptographic

signature. In accordance with some aspects, validating the second authorization ticket includes validating an identity of the second device as identified in the second authorization ticket. Additionally or alternatively, validation the second authorization ticket includes verifying possession of a private key associated with an identity and a public key included in a digital certificate and/or verifying a shared key derived though a mutual authentication process that occurred some time in the past between the devices.

[00136] Method 1000 can also include securing the validated communication session based on information contained in the first authorization ticket and the second authorization ticket. Securing the validated communication session includes encryption/decryption and integrity protection.

[00137] In accordance with some aspects, the first authorization ticket and/or the second authorization ticket are embodied as a traditional digital certificate. For example, the traditional digital certificate can be a X.509 standard with new extensions to indicate authorization for spectrum use and can convey information pertaining to setting up validated communication links. In another example, the traditional digital certificate can be a X.509 certificate that includes a new extension that contains an IP address.

[00138] With reference now to **Fig. 11**, illustrated is a method 1100 for spectrum authorization and access control. At 1102, a request for system access (*e.g.,* access to a licensed spectrum) is received from at least a first device. In accordance with some aspects, multiple requests from a number of devices are received at substantially the same time, at different times, or combinations thereof.

[00139] At 1104, authentication of the first device is obtained from an internal source, from and external source, or combinations thereof. If obtained externally, the authentication can be obtained from a network node over a secure communication link. In accordance with some aspects, the authentication is obtained externally from another server.

[00140] System access that can be authorized for the first device is determined, at 1106. In accordance with some aspects, determining system access includes consulting a configuration parameters database that contains a listing of a plurality of devices that are authorized to access the system.

[00141] The authentication of the first device, at 1104, and/or the authorized system access, at 1106, can be determined by credentials associated with the first

device. The credentials can be one or more of shared secret keys, public keys, authorization information, and a list of services or billing information, or combinations thereof.

[00142] At 1108, an authorization ticket for at least the first device is created based on the authorized system access to which the first device is entitled. The authorization ticket can include an identity of the first device, a validity range during which the authorization ticket is valid, and/or a cryptographic signature of the party that issued the authorization ticket.

[00143] **Fig. 12** illustrates a method 1200 for validating ticket-based configuration parameters. Method 1200 starts, at 1202, when a device is associated with one or more validated information elements. The information elements can include an Internet Protocol address assigned to the device, a telephone number assigned to the device, and/or other information.

[00144] In accordance with some aspects, prior to associating the device with the one or more information elements, an authorization protocol is employed to communicate with the device. Based in part on the communication with the device, a determination is made whether to construct an authorization ticket for the device and the information elements that should be included in the authorization ticket.

[00145] According to some aspects, a database of authorized devices and associated parameters identified by a unique device identifier is consulted to determine whether to associate the device with the information element(s). The database can contain information relating to a configuration each device can use when communicating using a licensed spectrum.

[00146] At 1204, an authorization ticket is transmitted to the device. The authorization ticket is certified by a trusted party and includes a subset of the one or more validated information elements. The device uses the authorization ticket to establish a communication link with another device. In accordance with some aspects, the authorization ticket includes an identifier of the device, a validity range, and a signature of the trusted party.

[00147] In accordance with some aspects, the authorization ticket is implemented as a traditional digital certificate. For example, the traditional digital certificate can be a X.509 standard with new extensions to indicate authorization for spectrum use and can convey information pertaining to setting up validated communication links. In another

example, the traditional digital certificate can be a X.509 certificate that includes a new extension that contains an IP address.

[00148] **Fig. 13** illustrates a method 1300 for validation of ticket-based configuration parameters. At 1302, an authorization ticket for a device (with which a validation communication session is to be established) is obtained. The authorization ticket can include one more validated information elements associated with the device. In accordance with some aspects, the authorization ticket includes an identifier of the device, a validity range, and a signature of a trusted party that issued the authorization ticket. At least one of the validated information elements is an Internet Protocol address. The authorization ticket is validated, at 1304.

[00149] The authorization ticket is utilized, at 1306, to establish a validated (and possibly secure) communication with the device. The communication can be broadcast or multicast. In accordance with some aspects, the validated communication with the device is a peer-to-peer configuration.

[00150] At 1308, a subset of the one or more validated information elements is used to perform a configuration operation. In accordance with some aspects, the configuration operation comprises configuring an interface. According to some aspect, the configuration operation comprises adding a route.

[00151] With reference now to **Fig. 14**, illustrated is a system 1400 that facilitates ticket based authorization and validation in accordance with the disclosed aspects. System 1400 can reside in a user device. System 1400 comprises a receiver 1402 that can receive a signal from, for example, a receiver antenna. The receiver 1402 can perform typical actions thereon, such as filtering, amplifying, downconverting, *etc.* the received signal. The receiver 1402 can also digitize the conditioned signal to obtain samples. A demodulator 1404 can obtain received symbols for each symbol period, as well as provide received symbols to a processor 1406.

[00152] Processor 1406 can be a processor dedicated to analyzing information received by receiver component 1402 and/or generating information for transmission by a transmitter 1408. In addition or alternatively, processor 1406 can control one or more components of user device 1400, analyze information received by receiver 1402, generate information for transmission by transmitter 1408, and/or control one or more components of user device 1400. Processor 1406 may include a controller component capable of coordinating communications with additional user devices. User device

1400 can additionally comprise memory 1408 operatively coupled to processor 1406 and that can store information related to coordinating communications and any other suitable information.

[00153] **Fig. 15** illustrates an example system 1500 that facilitates spectrum authorization and access control in an ad hoc (peer-to-peer) environment. System 1500 includes a logical grouping 1502 of electrical components that can act separately or in conjunction. Logical grouping 1502 includes an electrical component 1504 for obtaining a first authorization ticket for a first device. The first authorization ticket can be issued by a trusted third party. In accordance with some aspects, the trusted third party is an authorization server.

[00154] Also included in logical grouping 1502 is an electrical component 1506 for conveying the first authorization ticket to a second device. The first authorization ticket includes an identifier of the first device and a signature of the trusted third party. An electrical component 1508 for receiving from the second device a second authorization ticket for the second device is also included.

[00155] Logical grouping 1502 also includes an electrical component 1510 for validating the second authorization ticket for the second device. The second authorization ticket can include a validity time or a cryptographic signature of the issuer of the second authorization ticket (*e.g.,* trusted third party or another trusted party). Validating the second authorization ticket includes verifying both the validity time and the cryptographic signature. In accordance with some aspects, validating the second authorization ticket includes validating an identity of the second device as identified in the second authorization ticket, verifying possession of a private key associated with an identity and a public key included in a digital certification, or verifying a shared key derived through a mutual authentication process, or combinations thereof.

[00156] In accordance with some aspects, if there is a failure while validating the second authorization ticket for the second device, a communication link that was established between the first device and the second device is torn down. The communication link that is torn down is a non-validated link that the devices utilized to exchange authorization tickets and/or other information in order for a validated communication to be established.

[00157] An electrical component 1512 for establishing a validated communication session with the second device is also included in logical grouping

1502. The validated communication session can be configured to carry data of a type and manner specified in a list of allowed services included in the first authorization ticket, the second authorization ticket, or both tickets. In accordance with some aspects, the first authorization ticket includes services allowed to be accessed by the first device and the second authorization ticket comprises services allowed to be accessed by the second device.

[00158] Additionally, system 1500 can include a memory 1514 that retains instructions for executing functions associated with electrical components 1504, 1506, 1508, 1510, and 1512 or other components. While shown as being external to memory 1514, it is to be understood that one or more of electrical components 1504, 1506, 1508, 1510, and 1512 may exist within memory 1514.

[00159] **Fig. 16** illustrates an example system 1600 that provides spectrum authorization. Included in system is a logical grouping 1602 of electrical components that can act separately or in conjunction. Logical grouping 1602 includes an electrical component 1604 for receiving a request from at least a first device for access to a spectrum.

[00160] Also included in logical grouping 1602 is an electrical component 1606 for performing authentication of the at least a first device. The authentication can be performed using an internal source or an external source. In accordance with some aspects, the first device authentication is performed with the assistance of an external network device over a secure communication link.

[00161] An electrical component 1608 for determining system access that can be provided to the at least a first device is also included. In accordance with some aspects, electrical component 1608 determines system access by consulting a configuration parameters database that contains a listing of a plurality of devices that are authorized to access the system.

[00162] According to various aspects, electrical component 1606 can perform authentication and/or electrical component 1608 can determine spectrum access by reviewing credentials associated with the first device. The credentials can include one ore more shared secret keys, public keys, authorization information, a list of services, billing information, or combinations thereof.

[00163] Logical grouping 1602 further includes an electrical component 1610 for generating an authorization ticket for the at least a first device based in part on the

spectrum access that can be provided to the at least a first device. The authorization ticket can include an identity of the first device, a validity range during which the authorization ticket is valid, and/or a cryptographic signature.

[00164] In accordance with some aspects, logical grouping 1602 includes an electrical component (not shown) for transmitting the authorization ticket to the first device. In accordance with some aspects, multiple authorization tickets can be generated based on receipt of a multitude of requests. Each authorization ticket can be unique for each device and transmitted to each device individually.

[00165] System 1600 can also include a memory 1612 that retains instructions for executing functions associated with electrical components 1604, 1606, 1608, and 1610, or other components. While shown as being external to memory 1612, one or more of electrical components 1604, 1606, 1608, and 1610 can exist within memory 1612.

[00166] **Fig. 17** illustrates an example system 1700 that validates ticket-based configuration parameters in a communication environment. The communication environment can be in a peer-to-peer configuration or an ad-hoc configuration. Included in system 1700 is a logical grouping 1702 of electrical components that can act separately or in conjunction. Included in logical grouping 1702 is an electrical component 1704 for associating a device with one or more validated information elements. In accordance with some aspects, the information elements can be an Internet Protocol address assigned to the device and/or a telephone number assigned to the device.

[00167] Logical grouping 1702 also includes an electrical component 1706 for transmitting an authorization ticket certified by a trusted party to the device. The authorization ticket can include a cryptographic signature of the trusted party as well as other information (*e.g.,* device identifier, services to which a device can gain access, and so forth).

[00168] It should be noted that the process of validating the information elements is separate and distinct from the validation of authorization tickets. The trusted third party can obtain pre-validated information elements from another party or can validate the information elements itself through some other, separate process.

[00169] In accordance with some aspects, logical grouping 1702 includes an electrical component (not shown) for employing an authentication protocol or authorization protocol to communication with the device. Also included can be an

electrical component (not shown) for determining whether to construct an authorization ticket and which information elements to include in the authorization ticket. The determination can be made based in part on the communication with the device.

[00170] According to some aspects, logical grouping 1702 includes an electrical component (not shown) for consulting a database of authorized devices and associated parameters identified by a unique device identifier. The database can contain information related to a configuration each device can utilize when communicating using the licensed spectrum.

[00171] A memory 1708 that retains instructions for executing functions associated with electrical components 1704 and 1706 or other components is also included in system. Although an external memory 1708 is illustrated, in accordance with some aspects, one or more of electrical components 1704 and 1706 may exist within memory 1708.

[00172] With reference to **Fig. 18**, illustrated is an example system 1800 that validates ticket-based configuration parameters. System 1800 includes a logical grouping 1802 that includes an electrical component 1804 for acquiring an authorization ticket that includes one or more validated information elements associated with another device. In accordance with some aspects, at least one of the validated information elements is an Internet Protocol address.

[00173] Also included in logical grouping 1802 is an electrical component 1806 for validating the authorization ticket. The authorization ticket can include an identifier of the another device, a validity range, and a signature of a trusted party that issued the authorization ticket.

[00174] Logical grouping 1802 also includes an electrical component 1808 for establishing a validated communication with the another device based in part on the authorization ticket. The validated communication can be broadcast or multicast. The validated communication with the another device is a peer-to-peer configuration and/or an ad-hoc configuration.

[00175] An electrical component 1810 for performing a configuration operation with a subset of the one or more validated information elements is also included. The configuration operation can include configuring an interface and/or adding a route.

[00176] Additionally, system 1800 can include a memory 1812 that retains instructions for executing functions associated with electrical components 1804, 1806,

1808, and 1810 or other components. While shown as being external to memory 1812, it is to be understood that one or more of electrical components 1804, 1806, 1808, and 1810 can exist within memory 1812.

[00177] It is to be appreciated that the system 1500, 1600, 1700, and 1800 of Figs. 15, 16, 17, and 18, described above, are represented as including functional blocks, which may be functional blocks that represent functions implemented by a processor, software, or combination thereof (*e.g.,* firmware).

[00178] It is to be understood that the aspects described herein may be implemented by hardware, software, firmware or any combination thereof. When implemented in software, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Computer-readable media includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A storage media may be any available media that can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to carry or store desired program code means in the form of instructions or data structures and that can be accessed by a general-purpose or special-purpose computer, or a general-purpose or special-purpose processor. Also, any connection is properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, digital subscriber line (DSL), or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are included in the definition of medium. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk and blu-ray disc where *disks* usually reproduce data magnetically, while *discs* reproduce data optically with lasers. Combinations of the above should also be included within the scope of computer-readable media.

[00179] The various illustrative logics, logical blocks, modules, and circuits described in connection with the aspects disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an

application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but, in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, *e.g.*, a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration. Additionally, at least one processor may comprise one or more modules operable to perform one or more of the steps and/or actions described above.

[00180] For a software implementation, the techniques described herein may be implemented with modules (*e.g.*, procedures, functions, and so on) that perform the functions described herein. The software codes may be stored in memory units and executed by processors. The memory unit may be implemented within the processor or external to the processor, in which case it can be communicatively coupled to the processor through various means as is known in the art. Further, at least one processor may include one or more modules operable to perform the functions described herein.

[00181] The techniques described herein may be used for various wireless communication systems such as CDMA, TDMA, FDMA, OFDMA, SC-FDMA and other systems. The terms "system" and "network" are often used interchangeably. A CDMA system may implement a radio technology such as Universal Terrestrial Radio Access (UTRA), CDMA2000, *etc*. UTRA includes Wideband-CDMA (W-CDMA) and other variants of CDMA. Further, CDMA2000covers IS-2000, IS-95 and IS-856 standards. A TDMA system may implement a radio technology such as Global System for Mobile Communications (GSM). An OFDMA system may implement a radio technology such as Evolved UTRA (E-UTRA), Ultra Mobile Broadband (UMB), IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, Flash-OFDM®, *etc*. UTRA and E-UTRA are part of Universal Mobile Telecommunication System (UMTS). 3GPP Long Term Evolution (LTE) is a release of UMTS that uses E-UTRA, which employs OFDMA on the downlink and SC-FDMA on the uplink. UTRA, E-UTRA, UMTS, LTE and GSM are described in documents from an organization named "3rd Generation Partnership Project" (3GPP). Additionally, CDMA2000and UMB are described in

documents from an organization named "3rd Generation Partnership Project 2" (3GPP2). Further, such wireless communication systems may additionally include peer-to-peer (*e.g.*, mobile-to-mobile) *ad hoc* network systems often using unpaired unlicensed spectrums, 802.xx wireless LAN, BLUETOOTH and any other short- or long- range, wireless communication techniques.

[00182] Moreover, various aspects or features described herein may be implemented as a method, apparatus, or article of manufacture using standard programming and/or engineering techniques. The term "article of manufacture" as used herein is intended to encompass a computer program accessible from any computer-readable device, carrier, or media. For example, computer-readable media can include but are not limited to magnetic storage devices (*e.g.*, hard disk, floppy disk, magnetic strips, *etc.*), optical disks (*e.g.*, compact disk (CD), digital versatile disk (DVD), *etc.*), smart cards, and flash memory devices (*e.g.*, EPROM, card, stick, key drive, *etc.*). Additionally, various storage media described herein can represent one or more devices and/or other machine-readable media for storing information. The term "machine-readable medium" can include, without being limited to, wireless channels and various other media capable of storing, containing, and/or carrying instruction(s) and/or data. Additionally, a computer program product may include a computer readable medium having one or more instructions or codes operable to cause a computer to perform the functions described herein.

[00183] Further, the steps and/or actions of a method or algorithm described in connection with the aspects disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, a hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium may be coupled to the processor, such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. Further, in some aspects, the processor and the storage medium may reside in an ASIC. Additionally, the ASIC may reside in a user device. In the alternative, the processor and the storage medium may reside as discrete components in a user device. Additionally, in some aspects, the steps and/or actions of a method or algorithm may reside as one or any combination or set of codes and/or instructions on a

machine-readable medium and/or computer readable medium, which may be incorporated into a computer program product.

[00184] While the foregoing disclosure discusses illustrative aspects and/or aspects, it should be noted that various changes and modifications could be made herein without departing from the scope of the described aspects and/or aspects as defined by the appended claims. Accordingly, the described aspects are intended to embrace all such alterations, modifications and variations that fall within scope of the appended claims. Furthermore, although elements of the described aspects and/or aspects may be described or claimed in the singular, the plural is contemplated unless limitation to the singular is explicitly stated. Additionally, all or a portion of any aspect and/or aspect may be utilized with all or a portion of any other aspect and/or aspect, unless stated otherwise.

[00185] To the extent that the term "includes" is used in either the detailed description or the claims, such term is intended to be inclusive in a manner similar to the term "comprising" as "comprising" is interpreted when employed as a transitional word in a claim. Furthermore, the term "or" as used in either the detailed description of the claims is meant to be a "non-exclusive or".

CLAIMS

What is claimed is:

1. A method for validating ticket-based configuration parameters, comprising:

associating a device with one or more validated information elements; and

transmitting an authorization ticket certified by a trusted party to the device, the ticket includes a subset of the one or more validated information elements, wherein the device uses the authorization ticket to establish a communication link with another device.

2. The method of claim 1, wherein the validated information elements includes an Internet Protocol address assigned to the device.

3. The method of claim 1, wherein the validated information elements includes a telephone number assigned to the device.

4. The method of claim 1, wherein the authorization ticket includes a cryptographic signature of the trusted party.

5. The method of claim 1, further comprising:

employing an authentication protocol or authorization protocol to communicate with the device; and

determining whether to construct an authorization ticket and the information elements to include in the authorization ticket based in part on the communication with the device.

6. The method of claim 1, further comprises consulting a database of authorized devices and associated parameters identified by a unique device identifier, wherein the database contains information related to a configuration each device can use to communicate in a licensed spectrum.

7. The method of claim 1, wherein the authorization ticket includes an identifier of the device, a validity range, and a signature of the trusted party.

8. The method of claim 1, wherein the authorization ticket is implemented as a traditional digital certificate.

9. A wireless communications apparatus, comprising:

a memory that retains instructions related to associating a device with one or more validated information elements and transmitting an authorization ticket certified by a trusted party to the device, the ticket includes a subset of the one or more validated information elements, wherein the device uses the authorization ticket to establish a communication link with another device; and

a processor, coupled to the memory, configured to execute the instructions retained in the memory.

10. The wireless communications apparatus of claim 9, wherein the validated information elements include an Internet Protocol address assigned to the device, a telephone number assigned to the device, or both the Internet Protocol address and the telephone number.

11. The wireless communications apparatus of claim 9, the memory further retains instructions related to consulting a database of authorized devices and associated parameters identified by a unique device identifier, wherein the database contains information related to a configuration each device can use to communicate in a licensed spectrum.

12. The wireless communications apparatus of claim 9, the memory further retains instructions related to employing an authorization protocol to communicate with the device and determining whether to construct an authorization ticket and the information elements to include in the authorization ticket.

13. The wireless communications apparatus of claim 9, wherein the authorization ticket includes an identifier of the device, a validity range, and a signature of the trusted party.

14. A wireless communications apparatus that provides ticket-based validation parameters, comprising:

means for associating a device with one or more validated information elements; and

means for transmitting an authorization ticket certified by a trusted party to the device, the ticket includes a subset of the one or more validated information elements, wherein the device uses the authorization ticket to establish a validated and secure communication link with another device.

15. The wireless communications apparatus of claim 14, further comprising:

means for consulting a database of authorized devices and associated parameters identified by a device identifier, wherein the database contains information related to a configuration each device can use to communicate in a licensed spectrum.

16. The wireless communications apparatus of claim 14, wherein the authorization ticket includes an identifier of the device, a validity range, and a signature of the trusted party.

17. The wireless communications apparatus of claim 14, further comprising:

means for employing an authentication protocol to communicate with the device; and

means for determining whether to construct an authorization ticket and the information elements to include in the authorization ticket.

18. A computer program product, comprising:

a computer-readable medium comprising:

a first set of codes for causing a computer to communicate with a device;

a second set of codes for causing the computer to determine whether to create an authorization ticket for the device;

a third set of codes for causing the computer to associate the device with one or more validated information elements; and

a fourth set of codes for causing the computer to communicate the authorization ticket to the device, wherein the authorization ticket includes a subset of one or more validated information elements.

19. The computer program product of claim 18, wherein the authorization ticket includes an identifier of the device, a validity range, and a signature of a trusted party.

20. At least one processor configured to validate ticket-based configuration parameters, comprising:

a first module for consulting a database of authorized devices and associated parameters identified by a device identifier, wherein the database contains information related to a configuration each device can use to communicate in a licensed spectrum;

a second module for associating a device with one or more validated information elements; and

a third module for transmitting an authorization ticket certified by a trusted party to the device, the ticket includes a subset of the one or more validated information elements and the information related to the configuration the device can use to communicate, wherein the device uses the authorization ticket to establish a communication link with another device.

21. A method for validation of ticket-based configuration parameters, comprising:

obtaining an authorization ticket that includes one or more validated information elements associated with a device;

validating the authorization ticket;

utilizing the authorization ticket to establish a validated communication with the device; and

using a subset of the one or more validated information elements to perform a configuration operation.

22. The method of claim 21, wherein at least one of the validated information elements is an Internet Protocol address.

23. The method of claim 21, wherein the configuration operation comprises configuring an interface.

24. The method of claim 21, wherein the configuration operation comprises adding a route.

25. The method of claim 21, wherein the validated communication is broadcast or multicast.

26. The method of claim 21, wherein the authorization ticket includes an identifier of the device, a validity range, and a signature of a trusted party that issued the authorization ticket.

27. The method of claim 21, wherein the validated communication with the device is a peer-to-peer configuration.

28. A wireless communications apparatus, comprising:

a memory that retains instructions related to obtaining an authorization ticket that includes one or more validated information elements associated with a device, validating the authorization ticket, utilizing the authorization ticket to establish a validated communication with the device, and using a subset of the one or more validated information elements to perform a configuration operation; and

a processor, coupled to the memory, configured to execute the instructions retained in the memory.

29. The wireless communications apparatus of claim 28, wherein the authorization ticket includes an identifier of the device, a validity range, and a signature of a trusted party that issued the authorization ticket.

30. The wireless communications apparatus of claim 28, wherein the validated communication with the device is a peer to peer configuration.

31. The wireless communications apparatus of claim 28, wherein the configuration operation comprises at least one of configuring an interface or adding a route.

32. The wireless communications apparatus of claim 28, wherein the validated communication is broadcast or multicast.

33. A wireless communications apparatus that validates ticket-based configuration parameters, comprising:

means for acquiring an authorization ticket that includes one or more validated information elements associated with a device;

means for validating the authorization ticket;

means for establishing a validated communication with the device based in part on the authorization ticket; and

means for performing a configuration operation with a subset of the one or more validated information elements.

34. The wireless communications apparatus of claim 33, wherein the means for obtaining the authorization ticket requests the authorization ticket from a nearby device.

35. The wireless communications apparatus of claim 33, wherein the authorization ticket includes an identifier of the device, a validity range, and a signature of a trusted party that issued the authorization ticket.

36. The wireless communications apparatus of claim 33, wherein the validated communication with the device is an ad-hoc configuration.

37. A computer program product, comprising:

a computer-readable medium comprising:

a first set of codes for causing a computer to obtain an authorization ticket that includes one or more validated information elements associated with a device;

a second set of codes for causing the computer to validate the authorization ticket;

a third set of codes for causing the computer to utilize the authorization ticket to establish a validated communication with the device; and

a fourth set of codes for causing the computer to use a subset of the one or more validated information elements to perform a configuration operation.

38. The computer program product of claim 37, wherein the authorization ticket includes an identifier of the device, a validity range, and a signature of a trusted party that issued the authorization ticket.

39. At least one processor configured to provide spectrum authorization and access control, comprising:

a first module for acquiring an authorization ticket that includes one or more validated information elements associated with a device;

a second module for validating the authorization ticket;

a third module for employing the authorization ticket to establish a validated communication with the device; and

a fourth module for utilizing a subset of the one or more validated information elements to perform a configuration operation.

40. The at least one processor of claim 39, wherein the authorization ticket includes an identifier of the device, a validity range, and a signature of a trusted party that issued the authorization ticket.

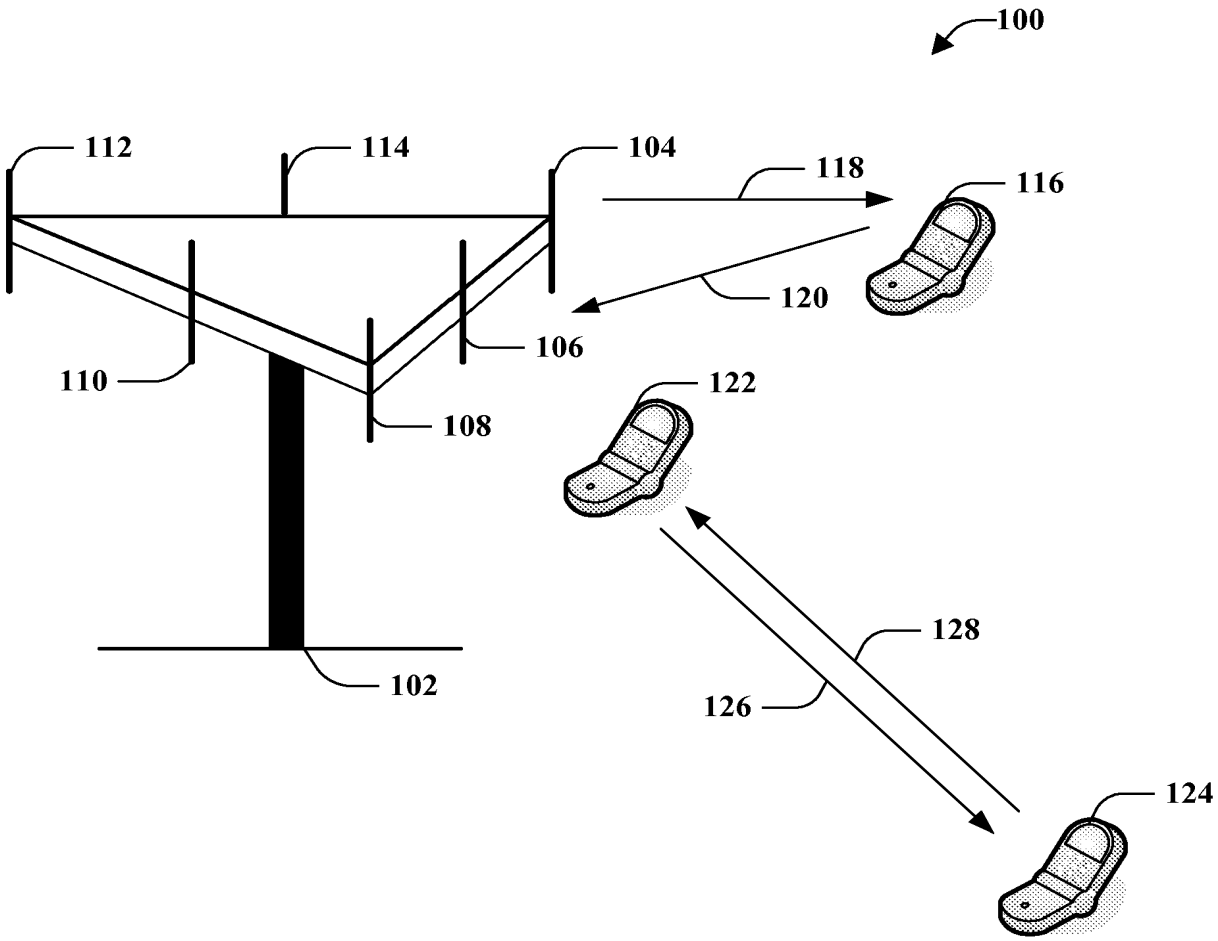


FIG. 1

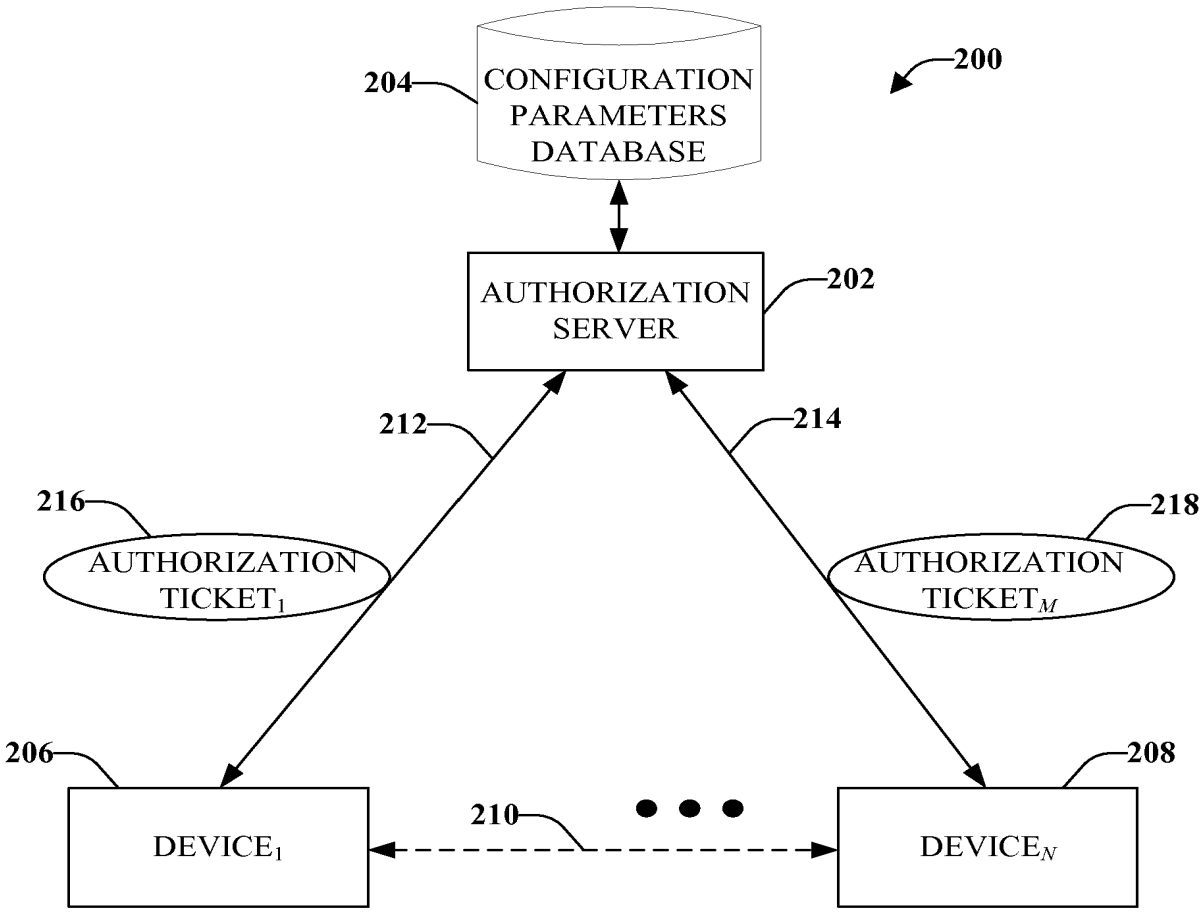

CONFIGURATION PARAMETERS DATABASE
204
200
AUTHORIZATION SERVER
202
212
214
216
AUTHORIZATION TICKET$_1$
218
AUTHORIZATION TICKET$_M$
206
208
210
DEVICE$_1$
DEVICE$_N$

FIG. 2

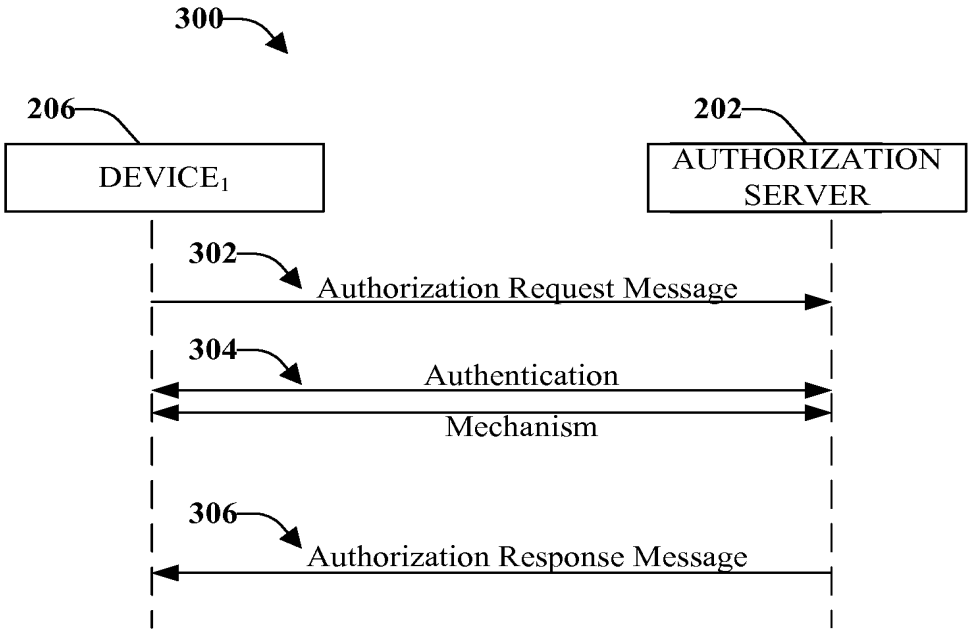

300
206
DEVICE1
202
AUTHORIZATION SERVER
302
Authorization Request Message
304
Authentication
Mechanism
306
Authorization Response Message

FIG. 3

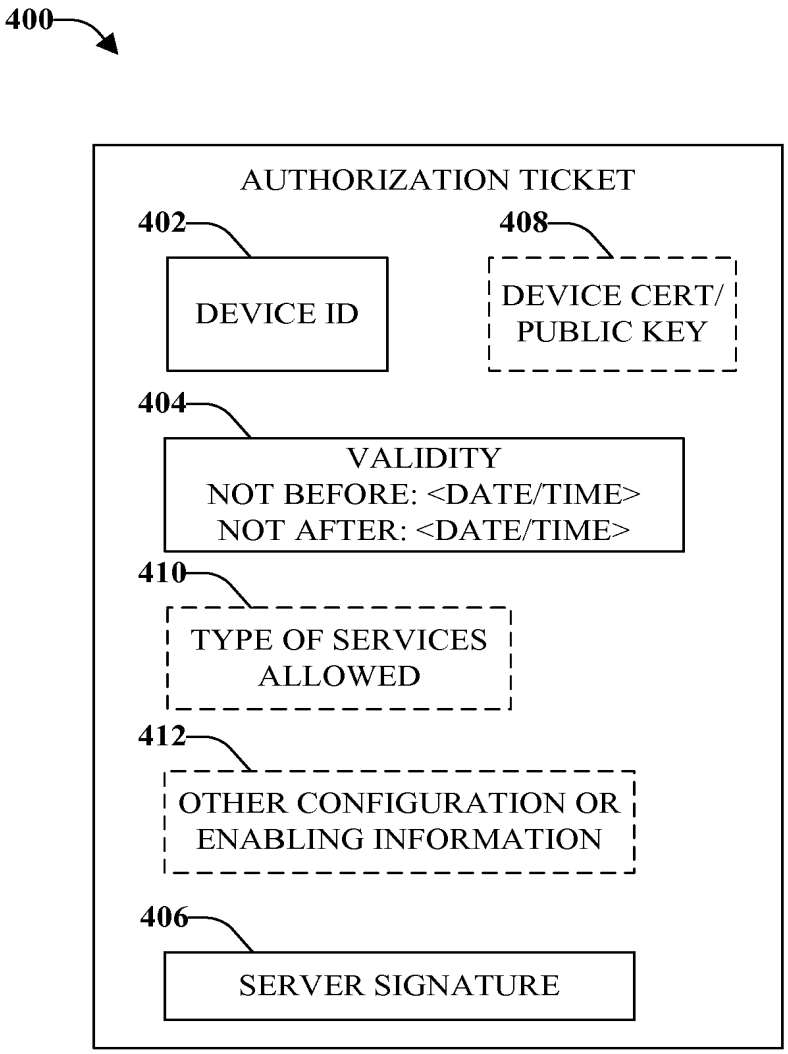

400
AUTHORIZATION TICKET
402
DEVICE ID
408
DEVICE CERT/
PUBLIC KEY
404
VALIDITY
NOT BEFORE: <DATE/TIME>
NOT AFTER: <DATE/TIME>
410
TYPE OF SERVICES
ALLOWED
412
OTHER CONFIGURATION OR
ENABLING INFORMATION
406
SERVER SIGNATURE

FIG. 4

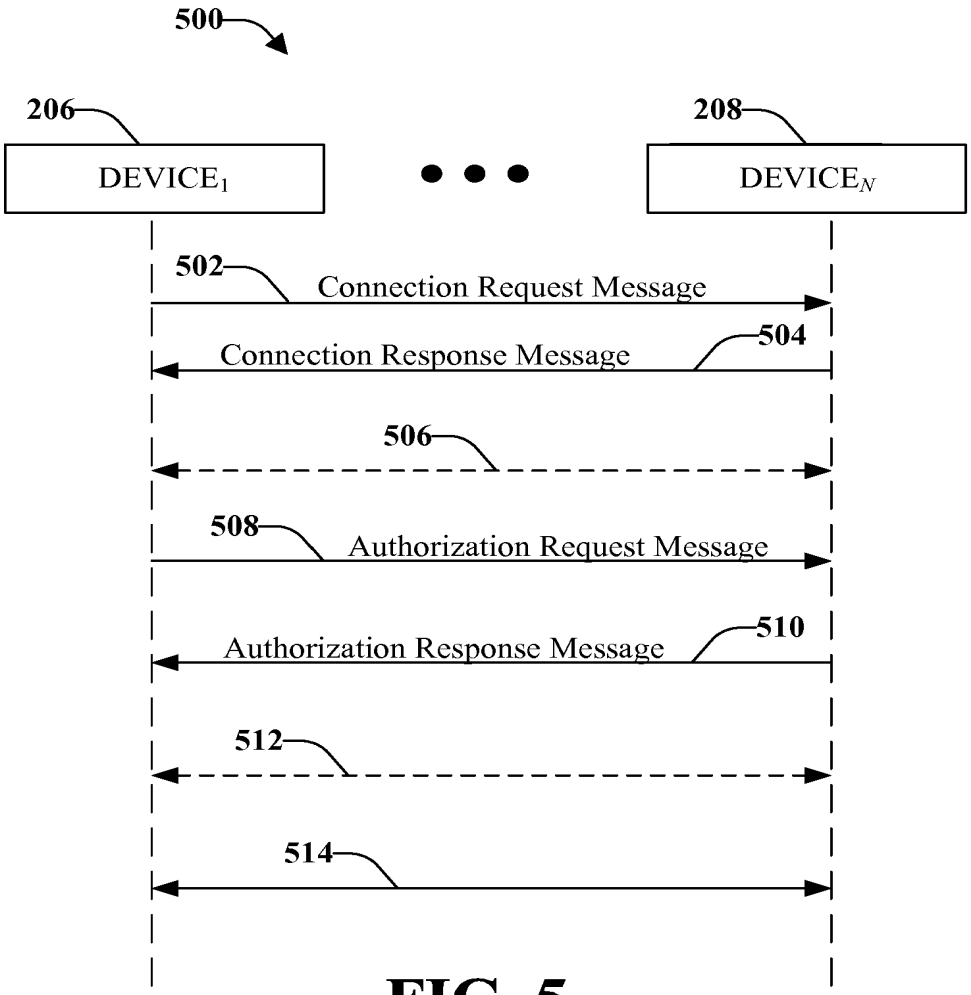

500
206
208
DEVICE1
DEVICEN
502
Connection Request Message
Connection Response Message
504
506
508
Authorization Request Message
Authorization Response Message
510
512
514

FIG. 5

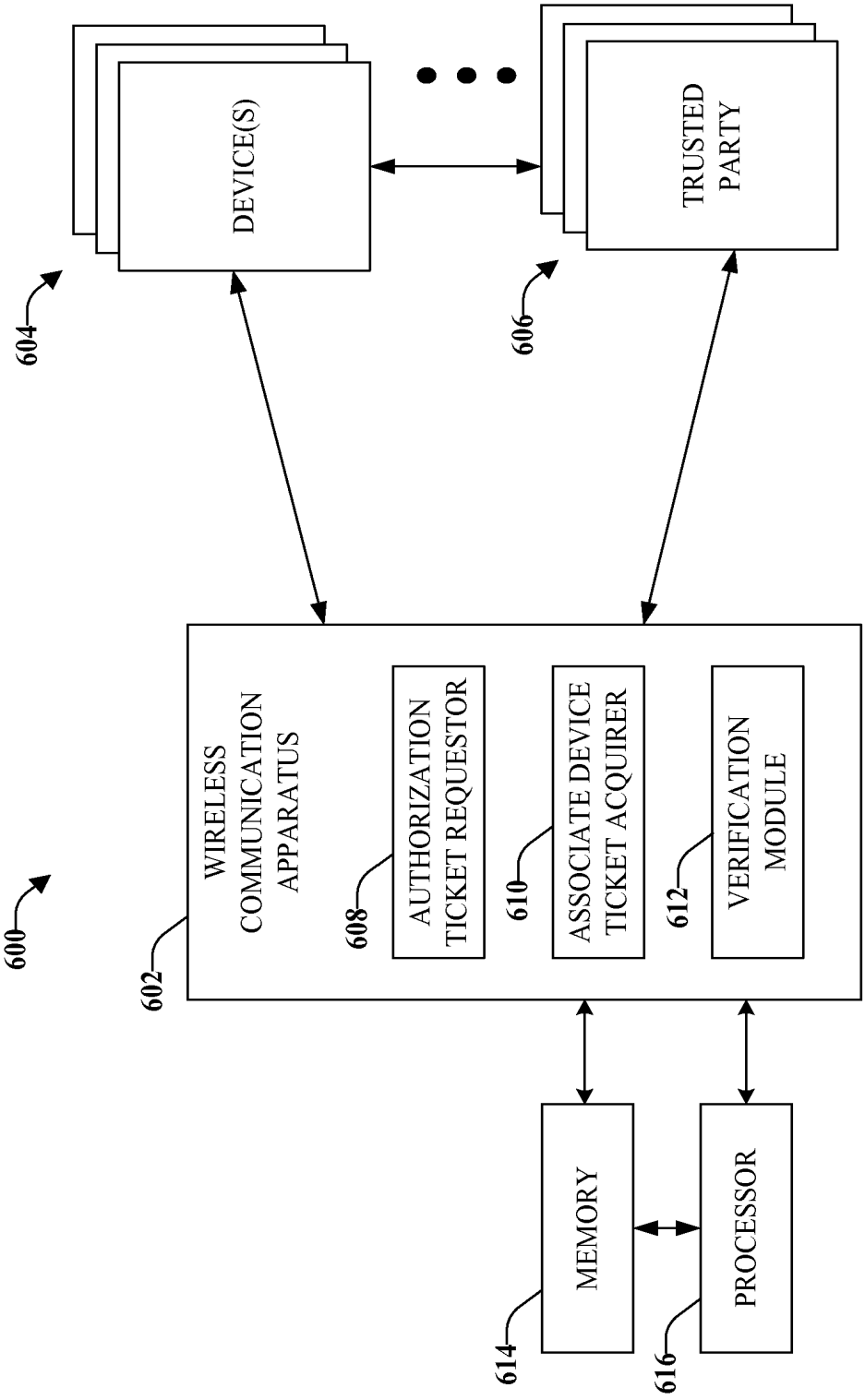

DEVICE(S)
TRUSTED PARTY
604
606
600
602
WIRELESS COMMUNICATION APPARATUS
608
AUTHORIZATION TICKET REQUESTOR
610
ASSOCIATE DEVICE TICKET ACQUIRER
612
VERIFICATION MODULE
614
MEMORY
616
PROCESSOR

FIG. 6

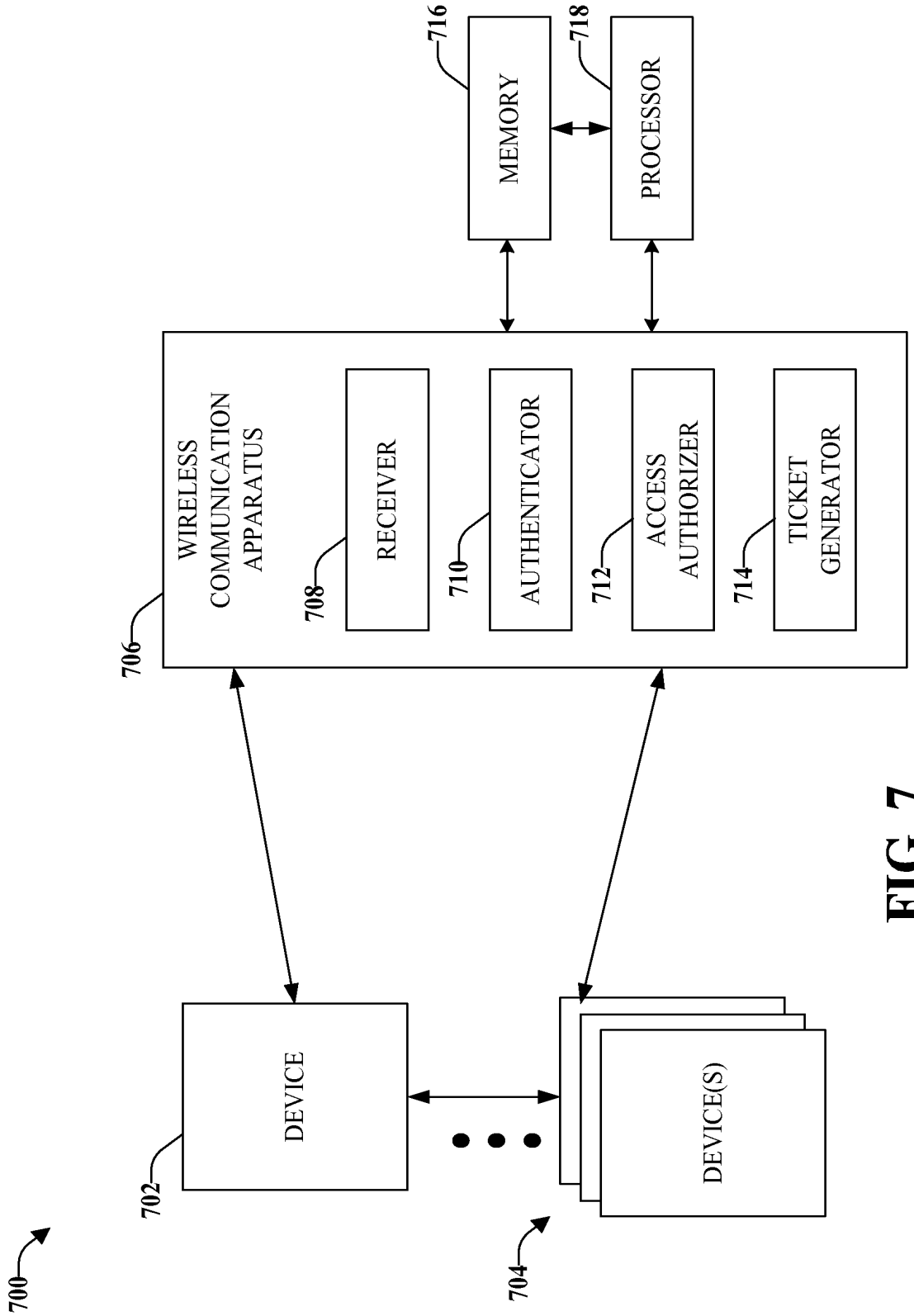

700
702
DEVICE
704
DEVICE(S)
706
WIRELESS COMMUNICATION APPARATUS
708
RECEIVER
710
AUTHENTICATOR
712
ACCESS AUTHORIZER
714
TICKET GENERATOR
716
MEMORY
718
PROCESSOR

FIG. 7

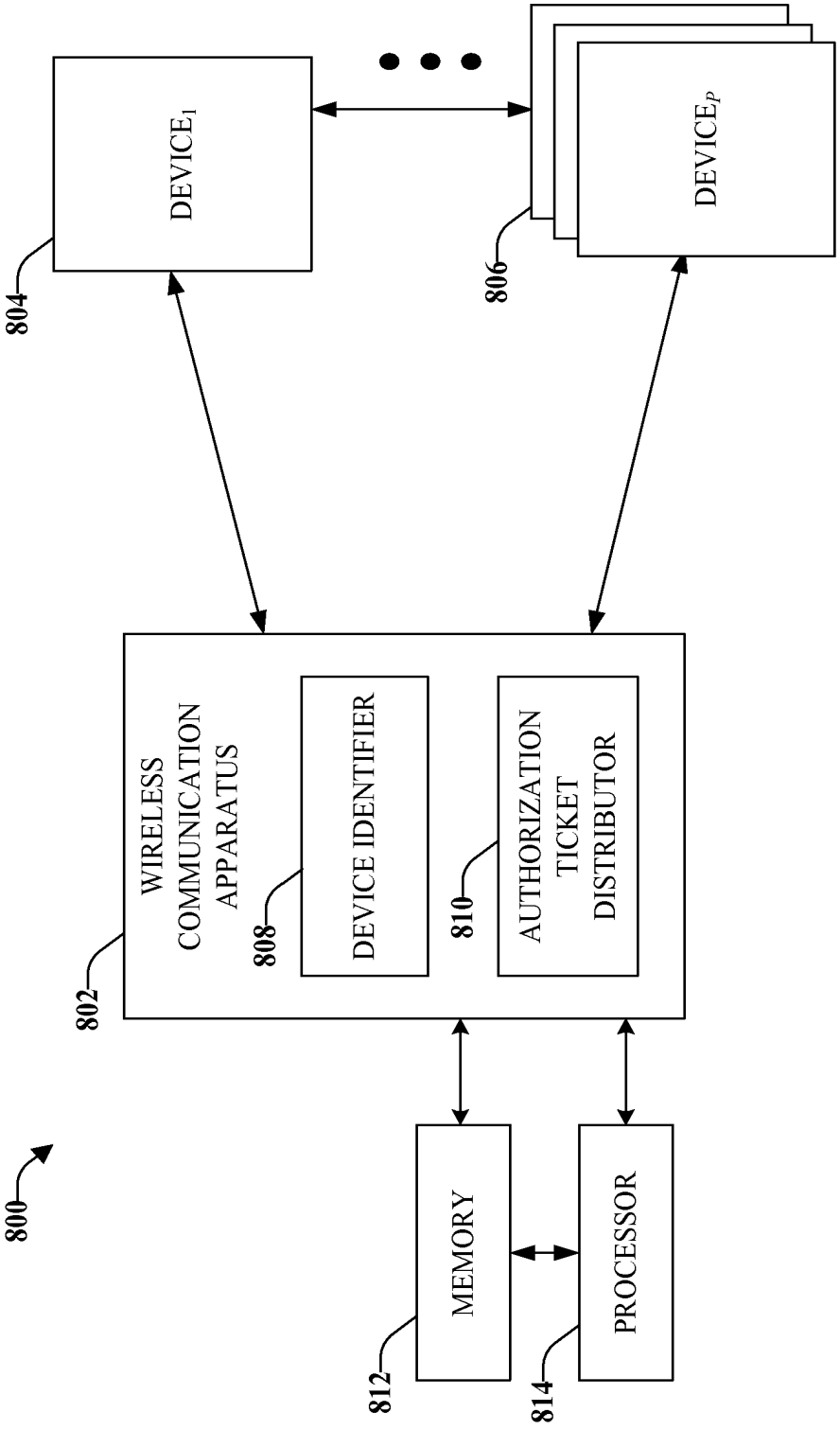

DEVICE1
DEVICEP
804
806
WIRELESS COMMUNICATION APPARATUS
802
DEVICE IDENTIFIER
808
AUTHORIZATION TICKET DISTRIBUTOR
810
MEMORY
812
PROCESSOR
814
800

FIG. 8

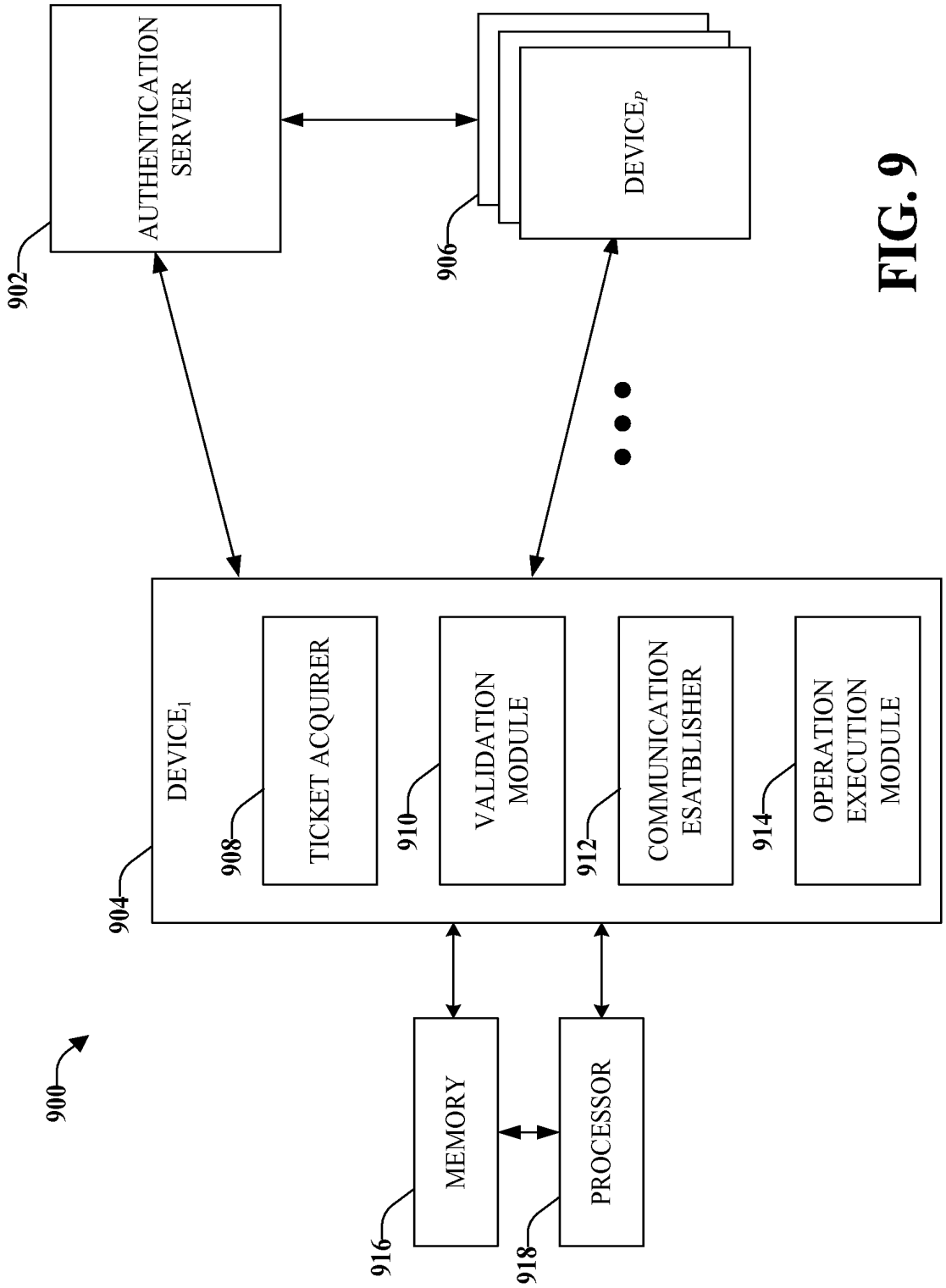

AUTHENTICATION SERVER
902
DEVICE$_P$
906
DEVICE$_1$
904
TICKET ACQUIRER
908
VALIDATION MODULE
910
COMMUNICATION ESATBLISHER
912
OPERATION EXECUTION MODULE
914
MEMORY
916
PROCESSOR
918
900

FIG. 9

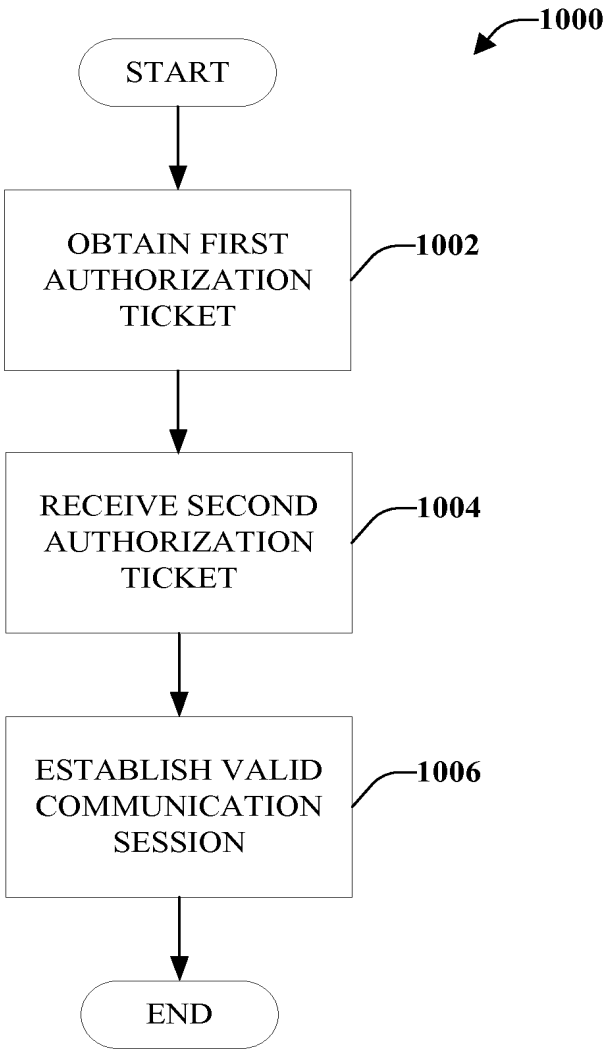

1000
START
OBTAIN FIRST AUTHORIZATION TICKET
1002
RECEIVE SECOND AUTHORIZATION TICKET
1004
ESTABLISH VALID COMMUNICATION SESSION
1006
END

FIG. 10

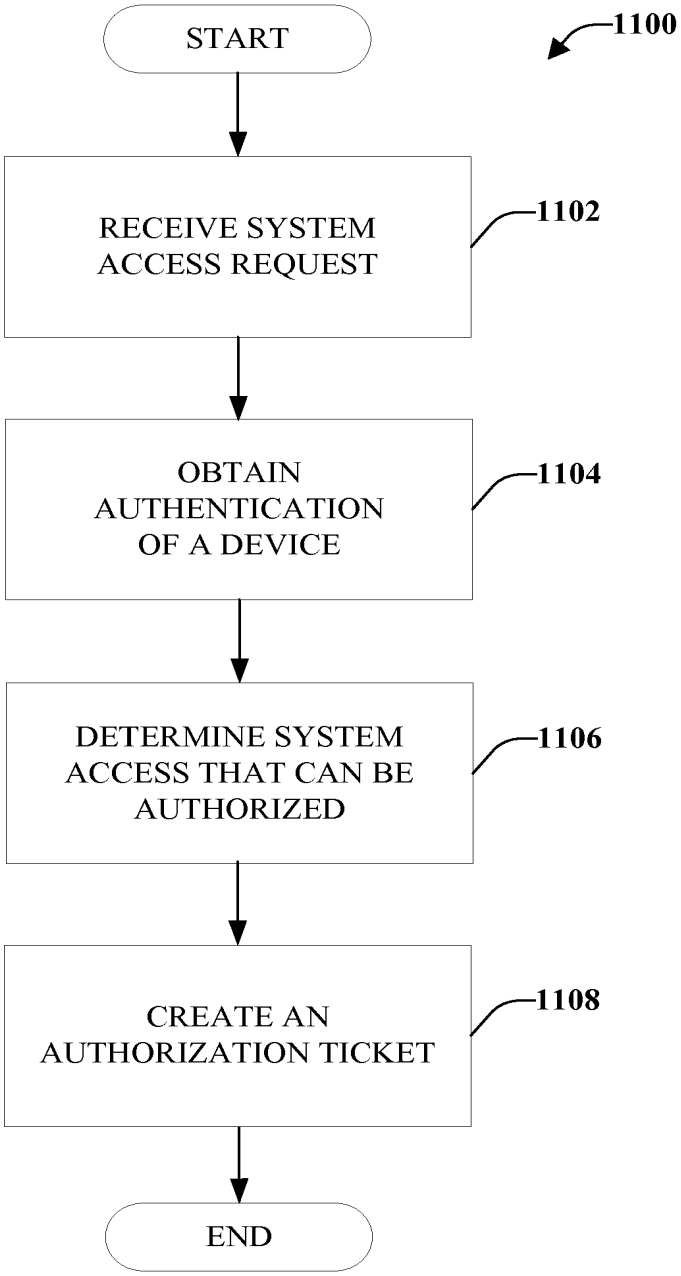

START
1100
RECEIVE SYSTEM ACCESS REQUEST
1102
OBTAIN AUTHENTICATION OF A DEVICE
1104
DETERMINE SYSTEM ACCESS THAT CAN BE AUTHORIZED
1106
CREATE AN AUTHORIZATION TICKET
1108
END

FIG. 11

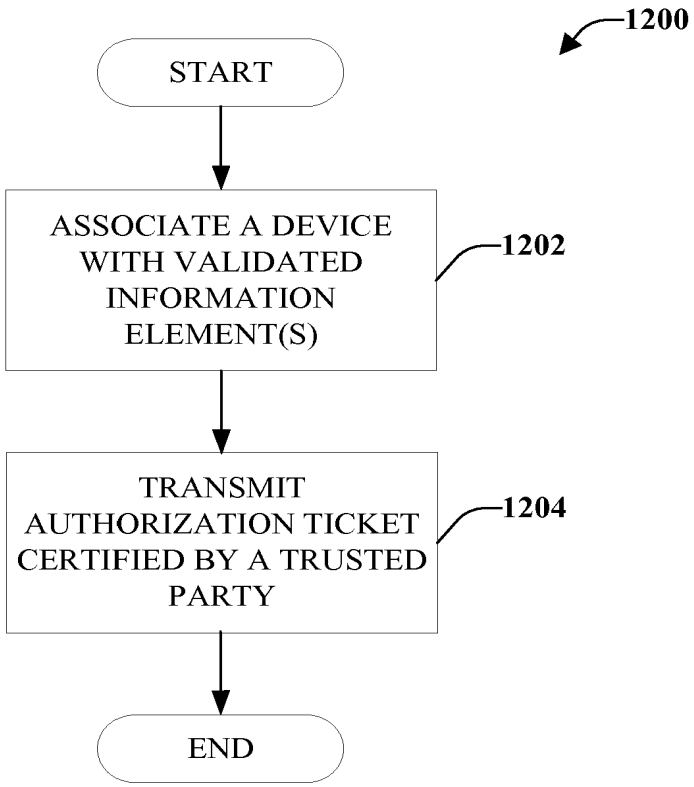

1200
START
ASSOCIATE A DEVICE WITH VALIDATED INFORMATION ELEMENT(S)
1202
TRANSMIT AUTHORIZATION TICKET CERTIFIED BY A TRUSTED PARTY
1204
END

FIG. 12

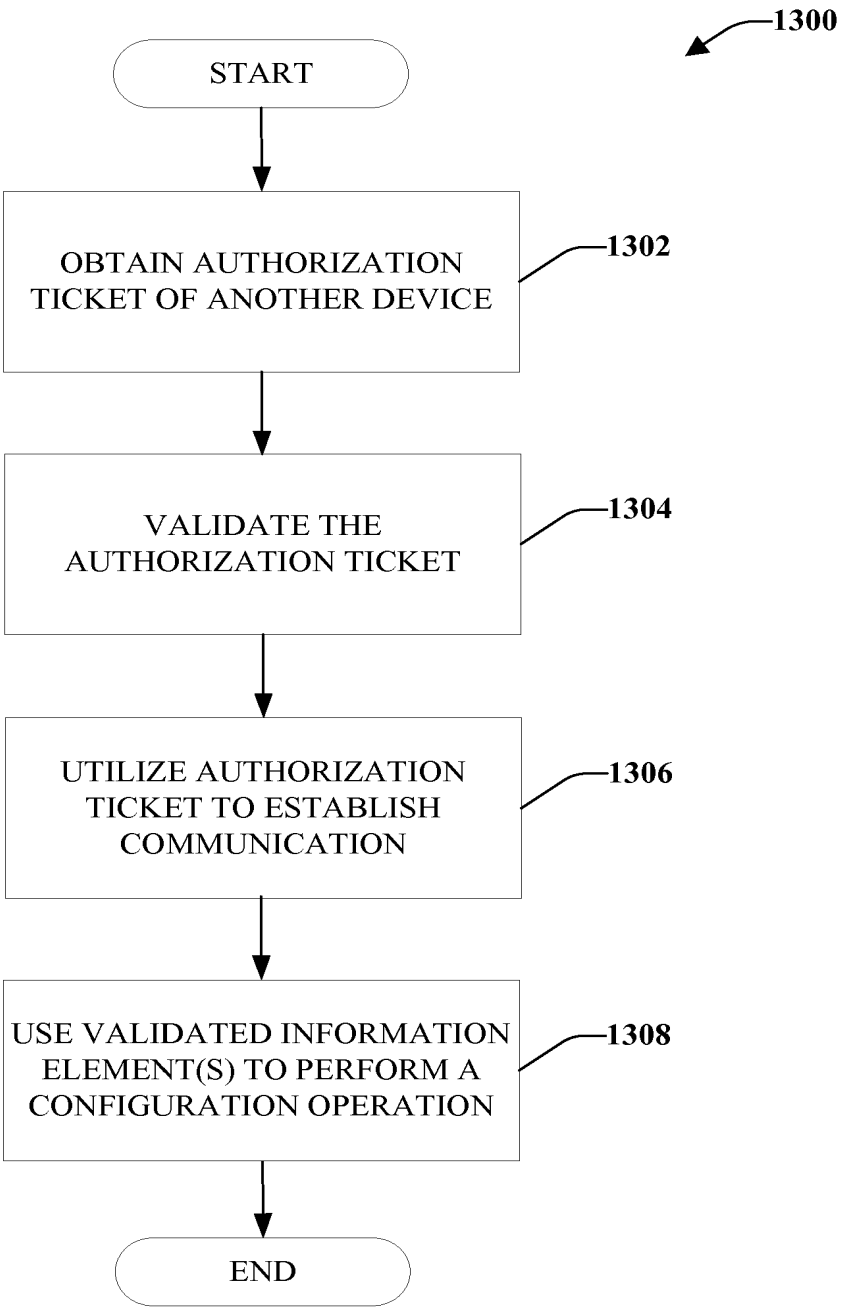

1300
START
OBTAIN AUTHORIZATION TICKET OF ANOTHER DEVICE
1302
VALIDATE THE AUTHORIZATION TICKET
1304
UTILIZE AUTHORIZATION TICKET TO ESTABLISH COMMUNICATION
1306
USE VALIDATED INFORMATION ELEMENT(S) TO PERFORM A CONFIGURATION OPERATION
1308
END

FIG. 13

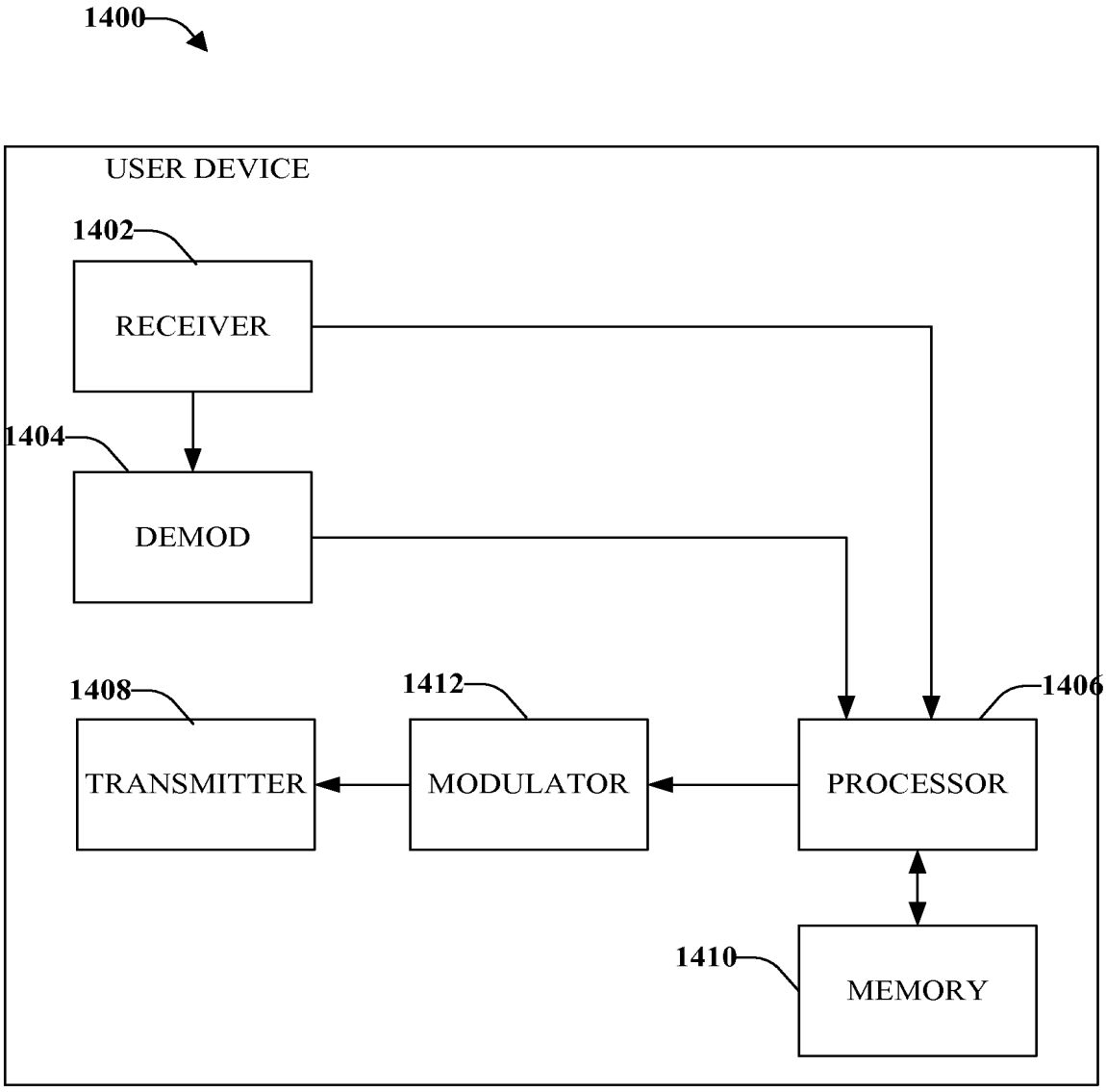

1400
USER DEVICE
1402
RECEIVER
1404
DEMOD
1408
TRANSMITTER
1412
MODULATOR
1406
PROCESSOR
1410
MEMORY

FIG. 14

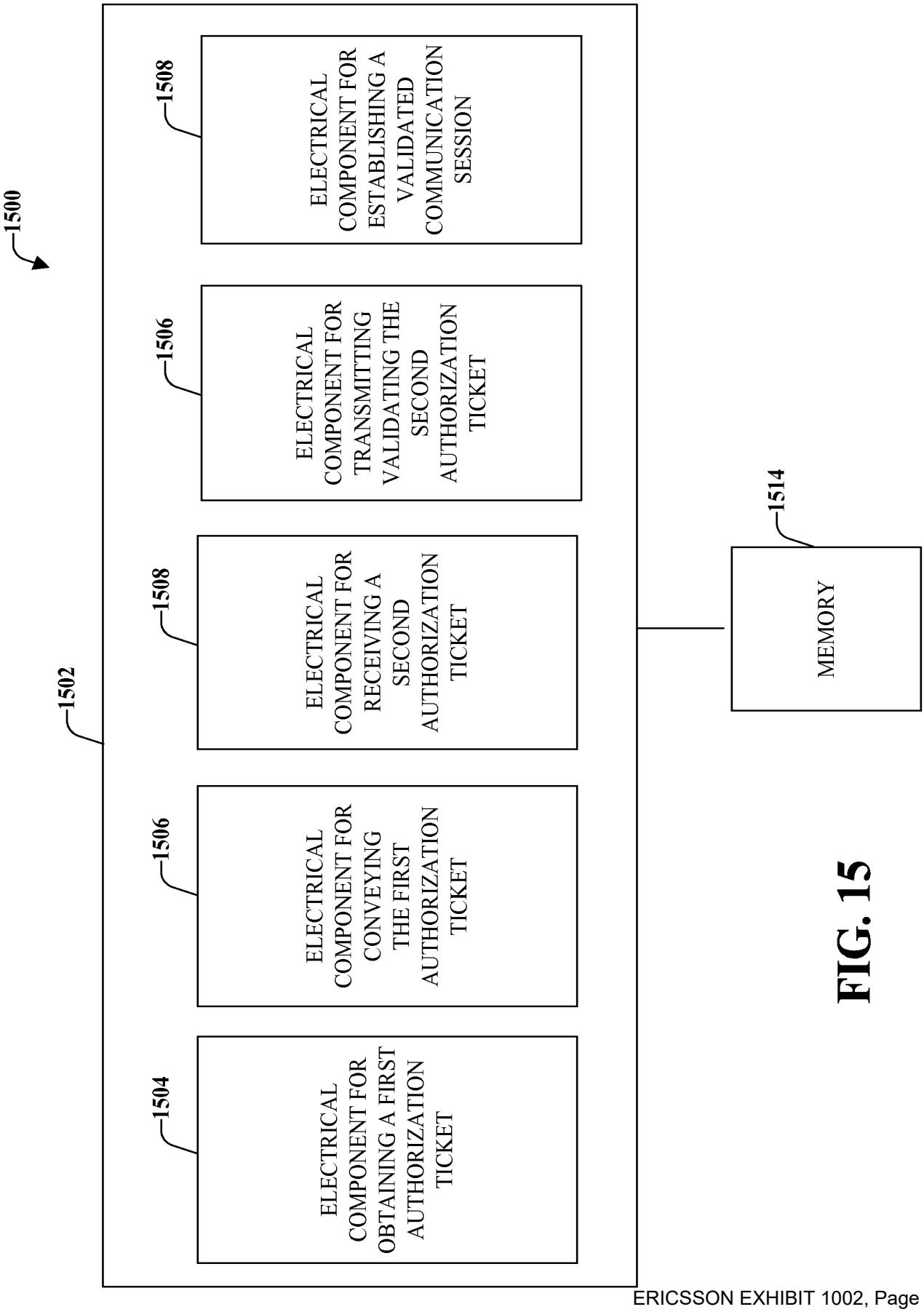

1500
1502
1504
ELECTRICAL COMPONENT FOR OBTAINING A FIRST AUTHORIZATION TICKET
1506
ELECTRICAL COMPONENT FOR CONVEYING THE FIRST AUTHORIZATION TICKET
1508
ELECTRICAL COMPONENT FOR RECEIVING A SECOND AUTHORIZATION TICKET
1506
ELECTRICAL COMPONENT FOR TRANSMITTING VALIDATING THE SECOND AUTHORIZATION TICKET
1508
ELECTRICAL COMPONENT FOR ESTABLISHING A VALIDATED COMMUNICATION SESSION
1514
MEMORY

FIG. 15

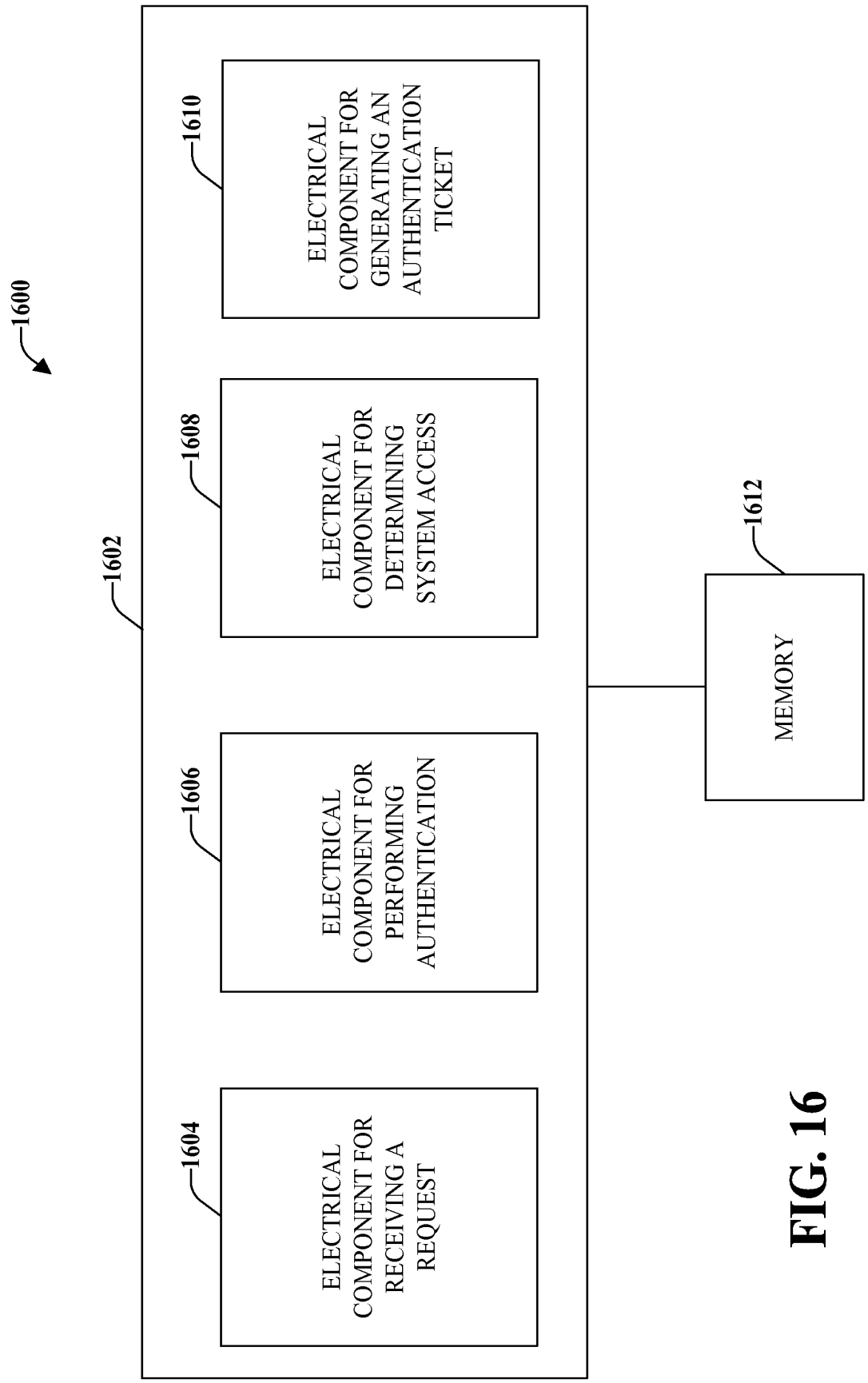

1600
1602
1604
ELECTRICAL COMPONENT FOR RECEIVING A REQUEST
1606
ELECTRICAL COMPONENT FOR PERFORMING AUTHENTICATION
1608
ELECTRICAL COMPONENT FOR DETERMINING SYSTEM ACCESS
1610
ELECTRICAL COMPONENT FOR GENERATING AN AUTHENTICATION TICKET
1612
MEMORY

FIG. 16

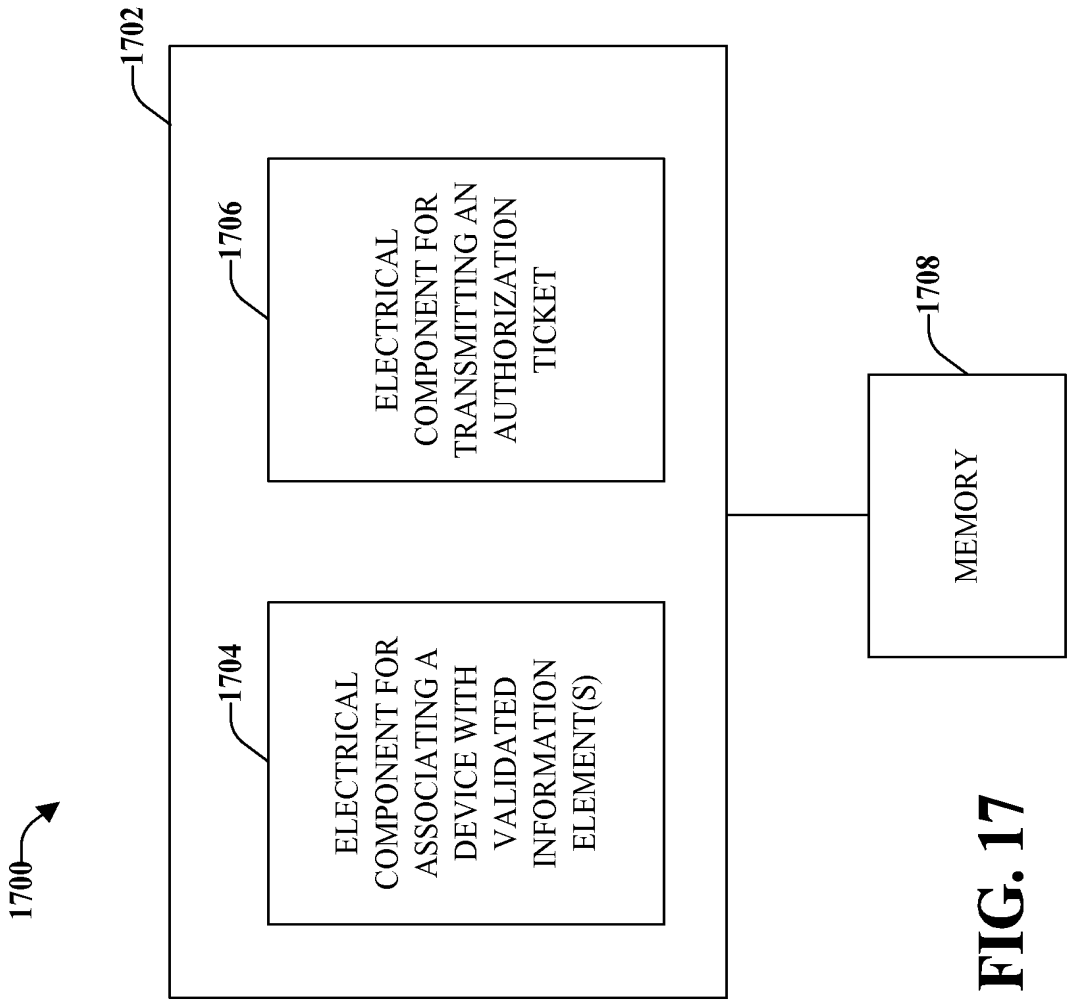

1700
1702
1704
ELECTRICAL COMPONENT FOR ASSOCIATING A DEVICE WITH VALIDATED INFORMATION ELEMENT(S)
1706
ELECTRICAL COMPONENT FOR TRANSMITTING AN AUTHORIZATION TICKET
1708
MEMORY

FIG. 17

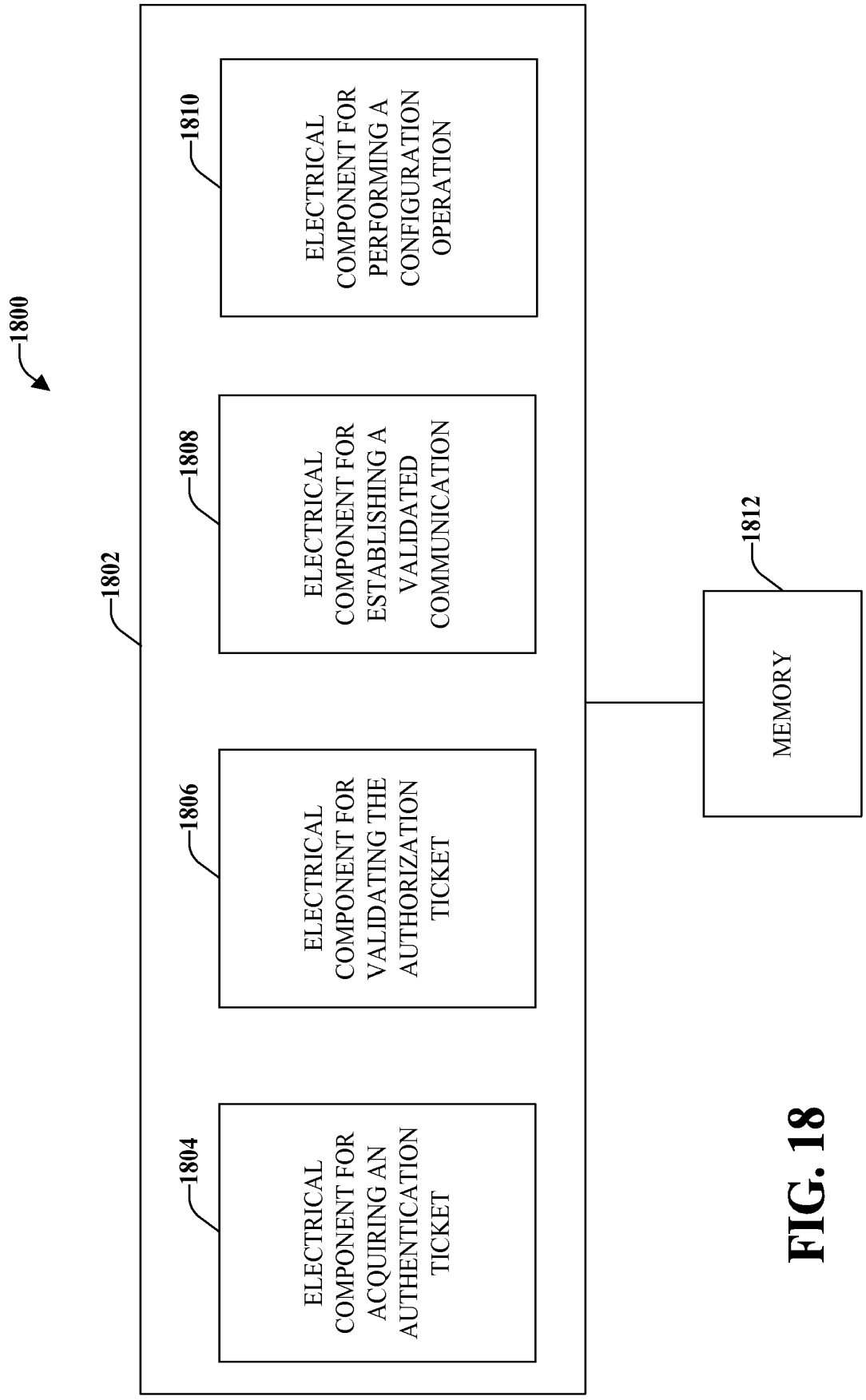

1800
1802
1804
ELECTRICAL COMPONENT FOR ACQUIRING AN AUTHENTICATION TICKET
1806
ELECTRICAL COMPONENT FOR VALIDATING THE AUTHORIZATION TICKET
1808
ELECTRICAL COMPONENT FOR ESTABLISHING A VALIDATED COMMUNICATION
1810
ELECTRICAL COMPONENT FOR PERFORMING A CONFIGURATION OPERATION
1812
MEMORY

FIG. 18

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 September 2011 (29.09.2011)

PCT

(10) International Publication Number
WO 2011/117677 A1

(51) International Patent Classification:
H04L 29/08 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/IB2010/051300

(22) International Filing Date:
24 March 2010 (24.03.2010)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI).

(71) Applicant *(for LC only)*: **NOKIA, INC.** [US/US]; 102 Corporate Park Dr., White Plains, New York 10604 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HAKOLA, Sami-Jukka** [FI/FI]; Peikontie 7, FI-90450 Kempele (FI). **KOSKELA, Timo** [FI/FI]; Rautatienkatu 50 as 5, FI-90120 Oulu (FI). **KOSKINEN, Henri Markus** [FI/FI]; Rummunlyöjänkatu 8 as 2, FI-02600 Espoo (FI).

(74) Agents: **QUIRK, Nathaniel T.** et al.; ALSTON & BIRD LLP, Bank of America Plaza, 101 S. Tryon Street, Suite 4000, Charlotte, NC 28280-4000 (US).

(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, TH, 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, LR, 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**: METHOD AND APPARATUS FOR DEVICE-TO-DEVICE KEY MANAGEMENT

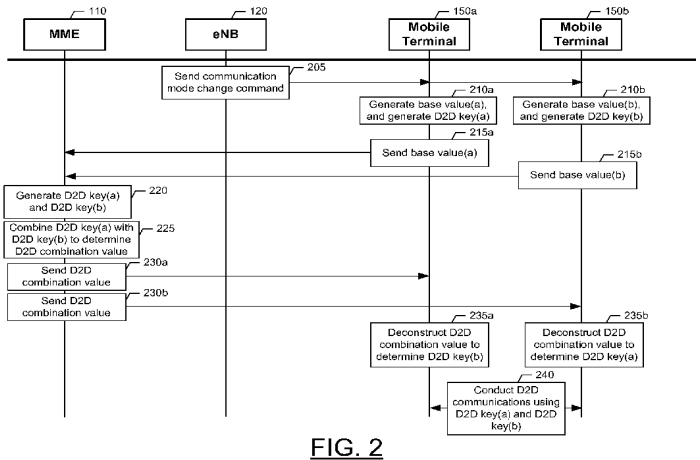


FIG. 2

(57) **Abstract**: Various methods for device-to-device key management are provided. One example method includes receiving a communication mode change command requesting a mode change to device-to-device communications, and generating a local device security key based on a secret key and a base value. The local device security key may be configured for use in device-to-device communications. The example method may also include receiving a security key combination value, and deconstructing the security key combination value using the local device security key to determine a peer device security key. The peer device security key may be configured for use in device-to- device communications. Similar and related example methods and example apparatuses are also provided.

WO 2011/117677 A1

METHOD AND APPARATUS FOR DEVICE-TO-DEVICE KEY MANAGEMENT

TECHNICAL FIELD

Embodiments of the present invention relate generally to communications, and, more particularly, relate to a method and apparatus device-to-device key management.

BACKGROUND

The modern communications era has brought about a tremendous expansion of wireless networks. Various types of networking technologies have been developed resulting in unprecedented expansion of computer networks, television networks, telephony networks, and the like, fueled by consumer demand within a wireless communications environment. Wireless and mobile networking technologies have addressed related consumer demands, while providing more flexibility and immediacy of information transfer.

With the continued evolution of wireless communications technology, wireless communications in a device-to-device setting have become increasingly practical. Via a device-to-device communications, a physical network need not be a conduit for communications between the devices. Rather, the devices, such as cellular devices, may directly communicate with each other, for example, to reduce the communications load on the physical network. However, communications security should be considered within a device-to-device setting.

BRIEF SUMMARY

Example methods and example apparatuses are described herein that provide for device-to-device key management. One example method includes receiving a communication mode change command requesting a mode change to device-to-device communications and generating a local device security key based on a secret key and a base value. The local device security key may be configured for use in device-to-device communications. The example method may also include receiving a security key combination value, and deconstructing the security key combination value using the local

device security key to determine a peer device security key. The peer device security key may also be configured for use in device-to-device communications.

An additional example embodiment is an apparatus configured for device-to-device key management. The example apparatus comprises at least one processor and at least one memory including computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to perform various functionality. The example apparatus may be caused to perform receiving a communication mode change command requesting a mode change to device-to-device communications and generating a local device security key based on a secret key and a base value. The local device security key may be configured for use in device-to-device communications. The example apparatus may also be caused to perform receiving a security key combination value, and deconstructing the security key combination value using the local device security key to determine a peer device security key. The peer device security key may also be configured for use in device-to-device communications.

Another example embodiment is a computer program product comprising a computer-readable storage medium having computer program code stored thereon, wherein execution of the computer program code causes an apparatus to perform various functionalities. Execution of the computer program code may cause an apparatus to perform receiving a communication mode change command requesting a mode change to device-to-device communications and generating a local device security key based on a secret key and a base value. The local device security key may be configured for use in device-to-device communications. Execution of the computer program code may also cause the apparatus to perform receiving a security key combination value, and deconstructing the security key combination value using the local device security key to determine a peer device security key. The peer device security key may also be configured for use in device-to-device communications.

Another example apparatus includes means for receiving a communication mode change command requesting a mode change to device-to-device communications and means for generating a local device security key based on a secret key and a base value. The local device security key may be configured for use in device-to-device communications. The example apparatus may also include means for receiving a security key combination value, and means for deconstructing the security key combination value using the local device security key to determine a peer device security key. The peer device security key may also be configured for use in device-to-device communications.

Another example method may include generating a first security key for a first device based on a first secret key and a first base value, where the first security key is configured for use in device-to-device communications from the first device. The example method may also include generating a second security key for a second device based on a second secret key and a second base value, where the second security key is also configured for use in device-to-device communications from the second device. The example method may further include combining the first security key with the second security key to generate a security key combination value, and causing sending of the security key combination value.

Another example apparatus comprises at least one processor and at least one memory including computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to perform various functionality. The example apparatus may be caused to perform generating a first security key for a first device based on a first secret key and a first base value, where the first security key is configured for use in device-to-device communications from the first device. The example apparatus may also be caused to perform generating a second security key for a second device based on a second secret key and a second base value, where the second security key is also configured for use in device-to-device communications from the second device. Further, the example apparatus may be caused to perform combining the first security key with the second security key to generate a security key combination value, and causing sending of the security key combination value.

Another example embodiment is a computer program product comprising a computer-readable storage medium having computer program code stored thereon, wherein execution of the computer program code causes an apparatus to perform various functionalities. Execution of the computer program code may cause an apparatus to perform generating a first security key for a first device based on a first secret key and a first base value, where the first security key is configured for use in device-to-device communications from the first device. Execution of the computer program code may also cause an apparatus to perform generating a second security key for a second device based on a second secret key and a second base value, where the second security key is also configured for use in device-to-device communications from the second device. Further, execution of the computer program code may also cause an apparatus to perform combining the first security key with the second security key to generate a security key combination value, and causing sending of the security key combination value.

Another example apparatus includes means for generating a first security key for a first device based on a first secret key and a first base value, where the first security key is configured for use in device-to-device communications from the first device. The example apparatus may also include means for generating a second security key for a second device based on a second secret key and a second base value, where the second security key is also configured for use in device-to-device communications from the second device. The example apparatus may further include means for combining the first security key with the second security key to generate a security key combination value, and means for causing sending of the security key combination value.

Another example method may include generating a first base value for determining a first security key for use with device-to-device communications from a first device, generating a second base value for determining a second security key for use with device-to-device communications from a second device, causing sending of a communication mode change command to the first device and the second device with the first base value and the second base value, causing sending of the first base value and the second base value to a key management network entity, and receiving a security key combination value from the key management network entity. The security key combination value may be a combination of the first security key and the second security key. The example method may also include causing sending of the security key combination value to the first device and the second device.

Another example apparatus comprises at least one processor and at least one memory including computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to perform various functionality. The example apparatus may be caused to perform generating a second base value for determining a second security key for use with device-to-device communications from a second device, causing sending of a communication mode change command to the first device and the second device with the first base value and the second base value, causing sending of the first base value and the second base value to a key management network entity, and receiving a security key combination value from the key management network entity. The security key combination value may be a combination of the first security key and the second security key. The example apparatus may also be caused to perform causing sending of the security key combination value to the first device and the second device.

Another example embodiment is a computer program product comprising a computer-readable storage medium having computer program code stored thereon, wherein execution of the computer program code causes an apparatus to perform various functionalities. Execution of the computer program code may cause an apparatus to

perform generating a second base value for determining a second security key for use with device-to-device communications from a second device, causing sending of a communication mode change command to the first device and the second device with the first base value and the second base value, causing sending of the first base value and the second base value to a key management network entity, and receiving a security key combination value from the key management network entity. The security key combination value may be a combination of the first security key and the second security key. Execution of the computer program code may also cause an apparatus to perform causing sending of the security key combination value to the first device and the second device.

Another example apparatus includes means for generating a first base value for determining a first security key for use with device-to-device communications from a first device, means for generating a second base value for determining a second security key for use with device-to-device communications from a second device, means for causing sending of a communication mode change command to the first device and the second device with the first base value and the second base value, means for causing sending of the first base value and the second base value to a key management network entity, and means for receiving a security key combination value from the key management network entity. The security key combination value may be a combination of the first security key and the second security key. The example apparatus may also include means for causing sending of the security key combination value to the first device and the second device.

BRIEF DESCRIPTION OF THE DRAWING(S)

Having thus described example embodiments of the invention in general terms, reference will now be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

FIG. 1 illustrates a communications system according to an example embodiment of the present invention;

FIG. 2 illustrates a flowchart and signaling diagram for device-to-device key management according to an example embodiment of the present invention;

FIG. 3 illustrates a flowchart and signaling diagram for device-to-device key management according to another example embodiment of the present invention;

FIG. 4 illustrates a flowchart and signaling diagram for device-to-device key management according to another example embodiment of the present invention;

FIG. 5 illustrates a block diagram of an apparatus and associated system for device-to-device key management according to an example embodiment of the present invention;

FIG. 6 illustrates a block diagram of a mobile terminal configured for device-to-device key management according to an example embodiment of the present invention; and
FIG. 7 illustrates a flow chart of a method for device-to-device key management according to an example embodiment of the present invention;
FIG. 8 illustrates a flow chart of another method for device-to-device key management according to an example embodiment of the present invention; and
FIG. 9 illustrates a flow chart of another method for device-to-device key management according to an example embodiment of the present invention.

DETAILED DESCRIPTION

Example embodiments of the present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all embodiments of the invention are shown. Indeed, the invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Like reference numerals refer to like elements throughout. The terms "data," "content," "information," and similar terms may be used interchangeably, according to some example embodiments of the present invention, to refer to data capable of being transmitted, received, operated on, and/or stored.

As used herein, the term 'circuitry' refers to all of the following: (a) hardware-only circuit implementations (such as implementations in only analog and/or digital circuitry); (b) to combinations of circuits and software (and/or firmware), such as (as applicable): (i) to a combination of processor(s) or (ii) to portions of processor(s)/software (including digital signal processor(s)), software, and memory(ies) that work together to cause an apparatus, such as a mobile phone or server, to perform various functions); and (c) to circuits, such as a microprocessor(s) or a portion of a microprocessor(s), that require software or firmware for operation, even if the software or firmware is not physically present.

This definition of 'circuitry' applies to all uses of this term in this application, including in any claims. As a further example, as used in this application, the term "circuitry" would also cover an implementation of merely a processor (or multiple processors) or portion of a processor and its (or their) accompanying software and/or firmware. The term "circuitry" would also cover, for example and if applicable to the particular claim element, a baseband integrated circuit or applications processor integrated circuit for a mobile phone or a similar integrated circuit in a server, a cellular network device, or other network device.

Various example embodiments of the present invention are directed to the generation, sharing, and utilization of security keys in the context of device-to-device (D2D) communications. D2D communications may be implemented in, for example, a cellular network, such as, for example, a Long Term Evolution (LTE)-based network. In D2D communications, the transmissions can be provided and received by wireless devices directly to or from each other at the physical layer, without using an access point or base station (e.g., evolved Node B (eNB)) as a conduit for communications.

An example of a D2D implementation in an LTE network involves the implementation of machine-to-machine (M2M) communications via LTE resources. In an example scenario, a device or mobile terminal may be connected to the LTE network, but may also act as a router for machines, sensors, or the like, that are equipped with an LTE radio but are not connected for example, to the evolved UMTS (Universal Mobile Telecommunications System) Terrestrial Radio Access Network (e-UTRAN) air interface. The machines or sensors may utilize D2D communications, for example, under LTE, to gain access to the LTE network through the device or mobile terminal.

In an LTE environment, both control and user plane data may be transmitted over an air interface using encrypted or secured connections. In this regard, the encryption or security may be realized via the use of user equipment (UE) (e.g., mobile terminal) specific and corresponding network side security or encryption keys. The keys may be generated from a secret or root key, such as an access security management entity key (K_{ASME}), that is, for example, known only by the UE and a mobility management entity (MME)/ home subscriber server (HSS). In non-D2D communications schemes, the encryption keys are not transmitted over an air interface for security purposes.

To support D2D communications in a secure fashion, similar techniques may be implemented. For example, each of the D2D devices may generate or acquire a security key for itself and for another device and cipher communications using its own D2D security key, while also deciphering communications provided by another device using the other device's D2D security key. However, according to some example embodiments, for security purposes each respective UE may generate or obtain the D2D security key of another device, without transmitting the D2D security key over an air interface. As such, various example embodiments of the present invention, describe mechanisms for sharing D2D security keys, while also avoiding the transmission of the D2D security keys via an air interface.

FIG. 1 illustrates an example communications system 100. The system 100 may support an LTE communications environment via e-UTRAN and D2D connections. The communications system 100 includes a mobility management entity (MME) 110, an evolved Node B (eNB 120), and mobile terminals 150a and 150b. The MME 110 may

be a node (e.g., server) in, for example, an LTE network, that performs key control. In some example embodiments, the MME 110 also performs or facilitates the performance of user authentication, performs idle mode tracking of UEs (e.g., mobile terminals 150), performs paging procedures for retransmissions, facilitates the activation and deactivation of bearers, and selects the serving gateway for a UE at initial attachment and during handovers involving core network node relocation. The MME 110 may also be one type of key management network entity that handles security key management. The eNB 120 may be an example of a wireless access point that provides access to the cellular network via an air interface such as, for example, e-UTRAN. The eNB 120 may operate to support connections to the LTE network by the mobile terminals 150a and 150b. The mobile terminals 150 may be examples of UEs that are configured to support, for example, both cellular and D2D communications. In the communications network 100, mobile terminal 150a is depicted as having a network connection 125a with the eNB 120 and a D2D connection 175 with the mobile terminal 150b. Similarly, mobile terminal 150b is depicted as having a network connection 125b with the eNB 120 and a D2D connection 175 with the mobile terminal 150a.

FIGs. 2-4 illustrate various example embodiments of the present invention in the form flowchart signaling diagrams involving the operations of the MME 110, the eNB 120, and the mobile terminals 150. In this regard, the example embodiments described in FIGs. 2-4 are configured to support the generation and sharing of D2D security keys, in some example embodiments, without the transmission of a D2D security key via an air interface.

FIG. 2 illustrates one example embodiment for D2D key management where the MME distributes information used to share peer D2D security keys. At 205, the eNB 120 sends a communications mode change command to the mobile terminals 150 (either in separate or shared messages) to trigger the mobile terminals 150 to transition to a D2D communications session, and, for example begin to establish the D2D connection 175. According to some example embodiments, the mobile terminals may be transitioning from a cellular connection to a D2D connection. The communications mode change command may be provided by the eNB 120 in the form of a radio resource control (RRC) reconfiguration command.

In response to the mode change command, the mobile terminals 150 may be configured to generate base values and use the base values to generate respective D2D security keys at 210a and 210b. In this regard, mobile terminal 150a may be configured to generate a base $value_a$, which may be a random or pseudo-random number, and implement a key derivation function using a secret key (e.g., $K_{ASME,a}$) and the base $value_a$ to generate a D2D security key_a ($K_{D2D,a}$) for use with D2D communications originating

from mobile terminal 150a. In some example embodiments, the secret key may be unique to the particular UE, but known by the UE and the MME. Similarly, mobile terminal 150b may be configured to generate a base $value_b$, which may be a random or pseudo-random number, and implement a key derivation function using a secret key (e.g., $K_{ASME,b}$) and the base $value_b$ to generate a D2D security key_b ($K_{D2D,b}$) for use with D2D communications originating from mobile terminal 150b.

The mobile terminals 150, at 215a and 215b, may be configured to send their respective base values to the MME 110. The transmissions of the base values may be sent to the MME 110 as secured messages and/or via a secured connection between each mobile terminal 150 and the MME 110. In some example embodiments, only the base values are transmitted to the MME 110 and not the D2D security keys for security reasons. The transmissions of the base values may, according to some example embodiments, be received by the eNB 120 and the eNB 120 may be configured to inform the MME 110 about the incoming message that include the base values. Alternatively, the messages including a base value may also include an indication (e.g., a data indication) that a D2D connection is being prepared. In some example embodiments, the messages including the base values may also include indications of which UEs will be involved in the D2D connection.

In response to receiving the base values, the MME 110 may be configured to, at 220, generate D2D security key_a and D2D security key_b using the same secret key as used by the mobile terminals (e.g., $K_{ASME,n}$ where n indicates the UE) via, for example, a key derivation function. The MME 110 may also be configured to combine D2D security key_a with D2D security key_b to generate or determine a D2D security key combination value at 225. According to some example embodiments, the procedure for combining D2D security key_a with D2D security key_b may include performing an exclusive-or operation on the security keys. At 230a and 230b, the MME 110 may be configured to send the D2D security key combination value to mobile terminals 150. In this regard, according to some example embodiments, the MME 110 may send the D2D security key combination value to each of the mobile terminals 150 separately, via individualized, secured connections to each respective mobile terminal 150.

In response to receiving the D2D security key combination value, the mobile terminals 150 may be configured to deconstruct the D2D security key combination value to determine a peer device's D2D security key at 235a and 235b. In this regard, mobile terminal 150a may deconstruct the D2D security key combination value, using, for example, its own D2D security key_a, to determine a peer device's D2D security key (e.g., mobile terminal 150b's D2D security key_b). Similarly, mobile terminal 150b may deconstruct the D2D security key combination value, using, for example, its own D2D

security key$_b$, to determine a peer device's D2D security key (e.g., mobile terminal 150a's D2D security key$_a$). To deconstruct the D2D security key combination value, the mobile terminals 150 may be configured to perform an exclusive-or operation on the D2D security key combination value using the mobile terminal's own (local) security key to determine the D2D security key of a peer device. According to some example embodiments, the exclusive-or operations performed at the MME 110 and the mobile terminals 150 allow for information related to the D2D security keys to be transmitted over an air interface in a manner that may be decipherable only if a device has a D2D security key that was used in the combining process.

As a result, each mobile terminal 150 may be in possession of its own D2D security key and the D2D security key of a peer device, without having transmitted a security key over an air interface. Accordingly, the mobile terminals 150, at 240, may conduct communications using the D2D security keys. In this regard, a mobile terminal may use its local D2D security key to cipher outgoing communications and use the peer device's D2D security key to decipher incoming communications from the peer device.

FIG. 3 illustrates another example embodiment for D2D key management where the eNB distributes information used to share the peer D2D security keys. At 300, in response to a decision to transition mobile terminals 150 to a D2D connection, the eNB 120 may be configured to generate base values (e.g., base value$_a$ and base value$_b$), which may be random or pseudo-random numbers. The eNB 120 may be configured to subsequently send base value$_a$ to mobile terminal 150a and base value$_b$ to mobile terminal 150b, at 305a and 305b, respectively. The base values may be sent with a communication mode change command to trigger the mobile terminals 150 to transition to a D2D communications session, and, for example begin to establish the D2D connection 175. According to some example embodiments, the mobile terminals may be transitioning from a cellular connection to a D2D connection. The communications mode change command may be provided by the eNB 120 in the form of a radio resource control (RRC) reconfiguration command. Further, the mode change command may be provided in an individualized message for each mobile terminal 150.

The eNB 120 may also send the base values to the MME 110, at 310. In response to receiving the base values, the MME 110 may be configured to, at 320, generate D2D security key$_a$ and D2D security key$_b$ using the same secret key as used by the mobile terminals (e.g., $K_{ASME,n}$) via, for example, a key derivation function. The MME 110 may also be configured to combine D2D security key$_a$ with D2D security key$_b$ to generate or determine a D2D security key combination value at 325. According to some example embodiments, the procedure for combining D2D security key$_a$ with D2D security key$_b$ may include performing an exclusive-or operation on the security keys. At 330, the

MME 110 may be configured to send the D2D security key combination value to the eNB 120.

The mobile terminals 150 may also be configured to generate their respective D2D security keys. In response to the mode change command, the mobile terminals 150 may be configured to use the base values provided by the eNB 120 to generate respective D2D security keys at 315a and 315b, respectively. In this regard, mobile terminal 150a may be configured to implement a key derivation function using a secret key (e.g., $K_{ASME,a}$) and the base $value_a$, which may be a random or pseudo-random number, and generate a D2D security key_a ($K_{D2D,a}$) for use with D2D communications originating from mobile terminal 150a. In some example embodiments, the secret key may be unique to the particular UE, but known by the UE and the MME. Similarly, mobile terminal 150b may be configured to implement a key derivation function using a secret key (e.g., $K_{ASME,b}$) and the base $value_b$, which may be a random or pseudo-random number, and generate a D2D security key_b ($K_{D2D,b}$) for use with D2D communications originating from mobile terminal 150b.

In response to receiving the D2D security key combination value, the eNB 120, at 335a and 335b, may be configured to send the D2D security key combination value to mobile terminals 150. In this regard, according to some example embodiments, the eNB 120 may send the D2D security key combination value to each of the mobile terminals 150 separately via individualized, secured connections to each respective mobile terminal 150.

In response to receiving the D2D security key combination value, the mobile terminals 150 may be configured to deconstruct the D2D security key combination value to determine a peer device's D2D security key at 340a and 340b. In this regard, mobile terminal 150a may deconstruct the D2D security key combination value, using, for example, its own D2D security key, to determine a peer device's D2D security key (e.g., mobile terminal 150b's D2D security key). Similarly, mobile terminal 150b may deconstruct the D2D security key combination value, using, for example, its own D2D security key, to determine a peer device's D2D security key (e.g., mobile terminal 150a's D2D security key). To deconstruct the D2D security key combination value, the mobile terminals 150 may be configured to perform an exclusive-or operation on the D2D security key combination value using the mobile terminal's own (local) security key to determine the D2D security key of a peer device. According to some example embodiments, the exclusive-or operations performed at the MME 110 and the mobile terminals 150 allow for information related to the D2D security keys to be transmitted over an air interface in a manner that may be decipherable only if a device has a D2D security key that was used in the combining process.

As a result, each mobile terminal 150 may be in possession of its own D2D security key and the D2D security key of a peer device, without having transmitted a security key over an air interface. Accordingly, the mobile terminals 150, at 350, may conduct communications using the D2D security keys. In this regard, a mobile terminal may use its local D2D security key to cipher outgoing communications and use the peer device's D2D security key to decipher incoming communications from the peer device.

FIG. 4 illustrates another example embodiment for D2D key management where the eNB distributes information used to share the peer D2D security keys, and a reduction in signaling. At 400, the eNB 120 determines that the mobile terminals 150 should transition to a D2D connection, and the eNB 120 sends a request for D2D security keys to the MME 110. In response to the request from eNB 120, the MME 110, at 405, may be configured to generate the base values (e.g., base $value_a$ and base $value_b$), which may be random or pseudo-random numbers. At 410, the MME 110 may be configured to generate D2D security key_a and D2D security key_b using the same secret key as used by the mobile terminals (e.g., $K_{ASME,n}$) via, for example, a key derivation function. The MME 110 may also be configured to combine D2D security key_a with D2D security key_b to generate or determine a D2D security key combination value at 415. According to some example embodiments, the procedure for combining D2D security key_a with D2D security key_b may include performing an exclusive-or operation on the security keys. At 420, the MME 110 may be configured to send the base values (e.g., base $value_a$ and base $value_b$) and the D2D security key combination value to the eNB 120.

In response to receiving the D2D security key combination value, the eNB 120, at 425a and 425b, may be configured to send the D2D security key combination value and the respective base values to mobile terminals 150. In this regard, according to some example embodiments, the eNB 120 may send base $value_a$ and the D2D security key combination value to mobile terminal 150a via individualized, secured connection with a communication mode change command (e.g., RRC message) at 425a. At 425b, according to some example embodiments, the eNB 120 may send base $value_b$ and the D2D security key combination value to mobile terminal 150b via individualized, secured connection with a communication mode change command (e.g., RRC message). The communications mode change commands may trigger the mobile terminals 150 to transition to a D2D communications session, and, for example begin to establish the D2D connection 175. According to some example embodiments, the mobile terminals may be transitioning from a cellular connection to a D2D connection.

In response to receipt of the messages at 425a and 425b, the mobile terminals 150 may be configured to generate their respective D2D security keys. In this regard, the mobile terminals 150 may be configured to use the base values provided by the eNB

120 to generate respective D2D security keys at 430a and 430b, respectively. Mobile terminal 150a may be configured to implement a key derivation function using a secret key (e.g., $K_{ASME,a}$) and the base $value_a$, which may be a random or pseudo-random number, and generate a D2D security key_a ($K_{D2D,a}$) for use with D2D communications originating from mobile terminal 150a. In some example embodiments, the secret key may be unique to the particular UE, but known by the UE and the MME. Similarly, mobile terminal 150b may be configured to implement a key derivation function using a secret key (e.g., $K_{ASME,b}$) and the base $value_b$, which may be a random or pseudo-random number, and generate a D2D security key_b ($K_{D2D,b}$) for use with D2D communications originating from mobile terminal 150a.

The mobile terminals 150 may also be configured to deconstruct the D2D security key combination value to determine a peer device's D2D security key at 435a and 435b. In this regard, mobile terminal 150a may deconstruct the D2D security key combination value, using, for example, its own D2D security key_a, to determine a peer device's D2D security key (e.g., mobile terminal 150b's D2D security key_b). Similarly, mobile terminal 150b may deconstruct the D2D security key combination value, using, for example, its own D2D security key_b, to determine a peer device's D2D security key (e.g., mobile terminal 150a's D2D security key_a). To deconstruct the D2D security key combination value, the mobile terminals 150 may be configured to perform an exclusive-or operation on the D2D security key combination value using the mobile terminal's own (local) security key to determine the D2D security key of a peer device. According to some example embodiments, the exclusive-or operations performed at the MME 110 and the mobile terminals 150 allow for information related to the D2D security keys to be transmitted over an air interface in a manner that may be decipherable only if a device has a D2D security key that was used in the combining process.

As a result, each mobile terminal 150 may be in possession of its own D2D security key and the D2D security key of a peer device, without having transmitted a security key over an air interface. Accordingly, the mobile terminals 150, at 440, may conduct communications using the D2D security keys. In this regard, a mobile terminal may use its local D2D security key to cipher outgoing communications and use the peer device's D2D security key to decipher incoming communications from the peer device.

The description provided above and generally herein illustrates example methods, example apparatuses, and example computer program products for device-to-device key management. FIG. 5 depicts example apparatuses that are configured to perform various functionalities as described herein, such as those described with respect to operation and configuration of a key management network entity (e.g., MME 110), an access point (e.g., eNB 120), or a terminal (e.g., mobile terminals 150), as described with

respect to FIGs. 1-4. FIG. 6 may be configured to operate in accordance with one of the mobile terminals 150.

Referring now to FIG. 5, an example embodiment of the present invention is depicted as apparatus 500. Via different configurations of the D2D key manager 540, the apparatus 500 may be configured to perform the functionality of a key management network entity (e.g., MME 110), an access point (e.g., eNB 120), a terminal (e.g., mobile terminals 150), or combinations thereof. Apparatus 500 may, be embodied as, or included as a component of, a communications device with wired or wireless communications capabilities. In some example embodiments, the apparatus 500 may be part of a communications device, such as a stationary or a mobile communications terminal. As a stationary communications terminal, the apparatus 500 may be part of, or embodied as, a server, a computer, an access point (e.g., base station), communications switching device, or the like. As a mobile device, the apparatus 500 may be a mobile and/or wireless communications node such as, for example, a mobile and/or wireless server, computer, access point, communications switching device, handheld device (e.g., telephone, portable digital assistant (PDA), mobile television, gaming device, camera, video recorder, audio/video player, radio, and/or a global positioning system (GPS) device), any combination of the aforementioned, or the like. Regardless of the type of communications device, apparatus 500 may also include computing capabilities.

The example apparatus 500 includes or is otherwise in communication with a processor 505, a memory device 510, an Input/Output (I/O) interface 506, a communications interface 515, and a D2D key manager 540. The processor 505 may be embodied as various means for implementing the various functionalities of example embodiments of the present invention including, for example, a microprocessor, a coprocessor, a controller, a special-purpose integrated circuit such as, for example, an ASIC (application specific integrated circuit), an FPGA (field programmable gate array), or a hardware accelerator, processing circuitry or the like. According to one example embodiment, processor 505 may be representative of a plurality of processors, or one or more multiple core processors, operating in concert. Further, the processor 505 may be comprised of a plurality of transistors, logic gates, a clock (e.g., oscillator), other circuitry, and the like to facilitate performance of the functionality described herein. The processor 505 may, but need not, include one or more accompanying digital signal processors. In some example embodiments, the processor 505 is configured to execute instructions stored in the memory device 510 or instructions otherwise accessible to the processor 505. The processor 505 may be configured to operate such that the processor causes the apparatus 500 to perform various functionalities described herein.

Whether configured as hardware or via instructions stored on a computer-readable storage medium, or by a combination thereof, the processor 505 may be an entity capable of performing operations according to embodiments of the present invention while configured accordingly. Thus, in example embodiments where the processor 505 is embodied as, or is part of, an ASIC, FPGA, or the like, the processor 505 is specifically configured hardware for conducting the operations described herein. Alternatively, in example embodiments where the processor 505 is embodied as an executor of instructions stored on a computer-readable storage medium, the instructions specifically configure the processor 505 to perform the algorithms and operations described herein. In some example embodiments, the processor 505 is a processor of a specific device (e.g., a communications server) configured for employing example embodiments of the present invention by further configuration of the processor 505 via executed instructions for performing the algorithms, methods, and operations described herein.

The memory device 510 may be one or more computer-readable storage media that may include volatile and/or non-volatile memory. In some example embodiments, the memory device 510 includes Random Access Memory (RAM) including dynamic and/or static RAM, on-chip or off-chip cache memory, and/or the like. Further, memory device 510 may include non-volatile memory, which may be embedded and/or removable, and may include, for example, read-only memory, flash memory, magnetic storage devices (e.g., hard disks, floppy disk drives, magnetic tape, etc.), optical disc drives and/or media, non-volatile random access memory (NVRAM), and/or the like. Memory device 510 may include a cache area for temporary storage of data. In this regard, some or all of memory device 510 may be included within the processor 505.

Further, the memory device 510 may be configured to store information, data, applications, computer-readable program code instructions, and/or the like for enabling the processor 505 and the example apparatus 500 to carry out various functions in accordance with example embodiments of the present invention described herein. For example, the memory device 510 could be configured to buffer input data for processing by the processor 505. Additionally, or alternatively, the memory device 510 may be configured to store instructions for execution by the processor 505.

The I/O interface 506 may be any device, circuitry, or means embodied in hardware, software, or a combination of hardware and software that is configured to interface the processor 505 with other circuitry or devices, such as the communications interface 515. In some example embodiments, the processor 505 may interface with the memory 510 via the I/O interface 506. The I/O interface 506 may be configured to convert signals and data into a form that may be interpreted by the processor 505. The

I/O interface 506 may also perform buffering of inputs and outputs to support the operation of the processor 505. According to some example embodiments, the processor 505 and the I/O interface 506 may be combined onto a single chip or integrated circuit configured to perform, or cause the apparatus 500 to perform, various functionalities of the present invention.

The communication interface 515 may be any device or means embodied in either hardware, a computer program product, or a combination of hardware and a computer program product that is configured to receive and/or transmit data from/to a network 520 and/or any other device or module in communication with the example apparatus 500. The communications interface may be configured to communicate information via any type of wired or wireless connection, and via any type of communications protocol, such as communications protocol that support cellular communications. According to various example embodiments, the communication interface 515 is configured to support the transmission and reception of communications in cellular networks, such as, for example, in a Long Term Evolution (LTE) environment using, for example, an evolved UMTS (Universal Mobile Telecommunications System) Terrestrial Radio Access Network (e-UTRAN) air interface. In this regard, the communications interface 515 may be configured to support device-to-device communications in, for example, LTE-based networks. Processor 505 may also be configured to facilitate communications via the communications interface by, for example, controlling hardware included within the communications interface 515. In this regard, the communication interface 515 may include, for example, communications driver circuitry (e.g., circuitry that supports wired communications via, for example, fiber optic connections), one or more antennas, a transmitter, a receiver, a transceiver and/or supporting hardware, including, for example, a processor for enabling communications. Via the communication interface 515, the example apparatus 500 may communicate with various other network entities in a device-to-device fashion and/or via indirect communications via a base station, access point, server, gateway, router, or the like.

The D2D key manager 540 of example apparatus 500 may be any means or device embodied, partially or wholly, in hardware, a computer program product, or a combination of hardware and a computer program product, such as processor 505 implementing stored instructions to configure the example apparatus 500, memory device 510 storing executable program code instructions configured to carry out the functions described herein, or a hardware configured processor 505 that is configured to carry out the functions of the D2D key manager 540 as described herein. In an example embodiment, the processor 505 includes, or controls, the D2D key manager 540. The D2D key manager 540 may be, partially or wholly, embodied as processors similar to, but

separate from processor 505. In this regard, the D2D key manager 540 may be in communication with the processor 505. In various example embodiments, the D2D key manager 540 may, partially or wholly, reside on differing apparatuses such that some or all of the functionality of the D2D key manager 540 may be performed by a first apparatus, and the remainder of the functionality of the D2D key manager 540 may be performed by one or more other apparatuses.

The D2D key manager 540 may be configured to perform the functionality described with respect to FIGs. 1-4, or cause apparatus 500 to perform the functionality described with respect to FIGs. 1-4, according to various example embodiments. In this regard, for example, based on the configuration of the D2D key manager 540, the apparatus 500 may be configured to perform the functionality of a key management network entity (e.g., MME 110), an access point (e.g., eNB 120), or a terminal (e.g., mobile terminals 150).

Further, the apparatus 500 and the processor 505 may be configured to perform the following functionality via D2D key manager 540. In this regard, the D2D key manager 540 may be configured to cause the processor 505 and/or the apparatus 500 to perform various functionalities, such as those depicted in the flowcharts of FIGs. 7-9 and as generally described herein.

For example, with reference to FIG. 7, when the D2D key manager 540 is configured to cause the apparatus 500 to operate as a terminal, such as mobile terminals 150, D2D key manager 540 may be configured to perform the following functionality. The D2D key manager 540 may be configured to receive a communication mode change command requesting a mode change to device-to-device communications at 700. The D2D key manager 540 may also be configured to generate, at 710, a local device security key based on a secret key and a base value. The local device security key may be configured for use in device-to-device communications. The D2D key manager 540 may also be configured to receive a security key combination value, at 720, and deconstruct the security key combination value using the local device security key to determine a peer device security key at 730. The peer device security key may be configured for use in device-to-device communications.

According to some example embodiments, the D2D key manager 540 may be configured to generate the local device security key based on the secret key and the base value, where the base value is a random or pseudo-random number. Further, in some example embodiments, the D2D key manager 540 may be configured to generate or receive the base value (e.g., the base value may be received from a mobility management entity), and cause sending of the base value to a key management network entity, which may be a mobility management entity. In some example embodiments, the

D2D key manager 540 may be configured to implement an exclusive-or operation on the security key combination value to determine the peer device security key. Further, in some example embodiments, the D2D key manager 540 may be configured to receive the security key combination value via a dedicated, secure connection between the sending entity and a receiving entity. According to some example embodiments, the communication mode change command, the base value, and the security key combination value are received in a common message, or according to some example embodiments, the communication mode change command and the base value may be received in a common message individualized for the receiving entity. The D2D key manager 540 may also be configured to cipher outgoing device-to-device communications using the local device security key, and decipher incoming device-to-device communications using the peer device security key.

Further, for example, with reference to FIG. 8, when the D2D key manager 540 is configured to cause the apparatus 500 to operate as a key management network entity, such as MME 110, D2D key manager 540 may be configured to perform the following functionality. In this regard, the D2D key manager 540 may be configured to generate a first security key for a first device (e.g., mobile terminal 150a) based on a first secret key for the first device and a first base value at 800. The first security key may be configured for use in device-to-device communications from the first device. The D2D key manager 540 may also be configured to generate a second security key for a second device (e.g., mobile terminal 150b) based on a second secret key for the second device and a second base value at 810. The second security key may also be configured for use in device-to-device communications from the second device. The D2D key manager 540 may be further configured to combine the first security key with the second security key to generate a security key combination value at 820, and cause sending of the security key combination value at 830.

In some example embodiments, the D2D key manager 540 may be configured to generate the first security key based on the first base value and generate the second security key based on the second base value, where the first base value is a first random or pseudo-random number associated with the first device and the second base value is a second random or pseudo-random number associated with the second device. In some example embodiments, the D2D key manager 540 may be configured to receive the first base value from the first device, and receive the second base value from the second device. Alternatively, in some example embodiments, the D2D key manager 540 may be configured to generate the first base value and the second base value. Further, in some example embodiments, the D2D key manager 540 may be configured to combine the first security key with the second security key through an exclusive-or

operation. According to some example embodiments, the D2D key manager 540 may be configured to cause sending of the security key combination value to the first device and the second device for deconstruction, or to an access point. In some example embodiments, the D2D key manager 540 may be configured to receive a request for the first security key and the second security key, and cause sending of the first base value, the second base value, and the security key combination value to an access point. Further, for example, with reference to FIG. 9, when the D2D key manager 540 is configured to cause the apparatus 500 to operate as an access point, such as eNB 120, D2D key manager 540 may be configured to perform the following functionality. In this regard, the D2D key manager 540 may be configured to generate a first base value for determining a first security key for use with device-to-device communications from a first device at 900, generate a second base value for determining a second security key for use with device-to-device communications from a second device at 910, and cause sending of a communication mode change command to the first device and the second device with the first base value and the second base value at 920. Further the D2D key manager 540 may be configured to cause sending of the first base value and the second base value to a key management network entity at 930, and receive a security key combination value from the key management network entity, where the security key combination value is a combination of the first security key and the second security key. Further, the D2D key manager 540 may be configured to cause sending of the security key combination value to the first device and the second device at 950.

In some example embodiments, the D2D key manager 540 may be configured to cause sending of a first communication mode change command with the first base value in an individualized message for the first device, and cause sending of a second communication mode change command with the second base value in an individualized message for the second device. Further, in some example embodiments, the D2D key manager 540 may also be configured to cause sending of the security key combination value via a dedicated and secure connection with the first device, and cause sending of the security key combination value via a dedicated and secure connection with the second device.

Referring now to FIG. 6, a more specific example apparatus in accordance with various embodiments of the present invention is provided. The example apparatus of FIG. 6 is a mobile terminal 10 configured to communicate within a wireless network, such as a cellular communications network. The mobile terminal 10 may be configured to perform the functionality of the mobile terminals 150 and/or apparatus 500 as described herein. More specifically, the mobile terminal 10 may be caused to perform the functionality described with respect to mobile terminals 150 in FIGs. 1-4 and FIG. 7 via the processor

20. Processor 20 may be an integrated circuit or chip configured similar to the processor 205 together with, for example, the I/O interface 506. Further, volatile memory 40 and non-volatile memory 42 may configured to support the operation of the processor 20 as computer readable storage media.

The mobile terminal 10 may also include an antenna 12, a transmitter 14, and a receiver 16, which may be included as parts of a communications interface of the mobile terminal 10. The speaker 24, the microphone 26, the display 28 (which may be a touch screen display), and the keypad 30 may be included as parts of a user interface.

FIGs. 2-4 and 7-9 illustrate flowcharts of example systems, methods, and/or computer program products according to example embodiments of the invention. It will be understood that each operation of the flowcharts, and/or combinations of operations in the flowcharts, can be implemented by various means. Means for implementing the operations of the flowcharts, combinations of the operations in the flowchart, or other functionality of example embodiments of the present invention described herein may include hardware, and/or a computer program product including a computer-readable storage medium (as opposed to a computer-readable transmission medium which describes a propagating signal) having one or more computer program code instructions, program instructions, or executable computer-readable program code instructions stored therein. In this regard, program code instructions for performing the operations and functions of FIGs. 2-4 and 7-9 may be stored on a memory device, such as memory device 510, volatile memory 40, or volatile memory 42, of an example apparatus, such as example apparatus 500 or mobile terminal 10, and executed by a processor, such as the processor 505 or processor 20. As will be appreciated, any such program code instructions may be loaded onto a computer or other programmable apparatus (e.g., processor 505, memory device 510, or the like) from a computer-readable storage medium to produce a particular machine, such that the particular machine becomes a means for implementing the functions specified in the flowcharts' operations. These program code instructions may also be stored in a computer-readable storage medium that can direct a computer, a processor, or other programmable apparatus to function in a particular manner to thereby generate a particular machine or particular article of manufacture. The instructions stored in the computer-readable storage medium may produce an article of manufacture, where the article of manufacture becomes a means for implementing the functions specified in the flowcharts' operations. The program code instructions may be retrieved from a computer-readable storage medium and loaded into a computer, processor, or other programmable apparatus to configure the computer, processor, or other programmable apparatus to execute operations to be performed on or by the computer, processor, or other programmable apparatus. Retrieval, loading, and

execution of the program code instructions may be performed sequentially such that one instruction is retrieved, loaded, and executed at a time. In some example embodiments, retrieval, loading and/or execution may be performed in parallel such that multiple instructions are retrieved, loaded, and/or executed together. Execution of the program code instructions may produce a computer-implemented process such that the instructions executed by the computer, processor, or other programmable apparatus provide operations for implementing the functions specified in the flowcharts' operations.

Accordingly, execution of instructions associated with the operations of the flowchart by a processor, or storage of instructions associated with the blocks or operations of the flowcharts in a computer-readable storage medium, support combinations of operations for performing the specified functions. It will also be understood that one or more operations of the flowcharts, and combinations of blocks or operations in the flowcharts, may be implemented by special purpose hardware-based computer systems and/or processors which perform the specified functions, or combinations of special purpose hardware and program code instructions.

Many modifications and other embodiments of the inventions set forth herein will come to mind to one skilled in the art to which these inventions pertain having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the inventions are not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Moreover, although the foregoing descriptions and the associated drawings describe example embodiments in the context of certain example combinations of elements and/or functions, it should be appreciated that different combinations of elements and/or functions may be provided by alternative embodiments without departing from the scope of the appended claims. In this regard, for example, different combinations of elements and/or functions other than those explicitly described above are also contemplated as may be set forth in some of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving a communication mode change command requesting a mode change to device-to-device communications;

generating a local device security key based on a secret key and a base value, the local device security key being configured for use in device-to-device communications;

receiving a security key combination value; and

deconstructing the security key combination value using the local device security key to determine a peer device security key, the peer device security key being configured for use in device-to-device communications.

2. The method of claim 1, wherein generating the local device security key based on the secret key and the base value includes generating the local device security key based on the secret key and the base value, wherein the base value is a random or pseudo-random number.

3. The method of claim 1, further comprising generating the base value.

4. The method of claim 1 further comprising:

generating the base value; and

causing sending of the base value to a key management network entity.

5. The method of any one of claims 1 through 4, wherein receiving the security key combination value includes receiving the security key combination value from a mobility management entity.

6. The method of claim 1 further comprising:

generating the base value; and

causing sending of the base value to a key management network entity, the key management network entity being a mobility management entity.

7. The method of any one of claims 1 through 6, wherein deconstructing the security key combination value includes implementing an exclusive-or operation on the security key combination value to determine the peer device security key.

8. The method of any on of claims 1 through 7, wherein receiving the security key combination value includes receiving the security key combination value via a secure connection with the sending entity, the secure connection being a dedicated connection between the sending entity and a receiving entity.

9. The method of any one of claims 1 through 8, wherein the communication mode change command, the base value, and the security key combination value are received in a common message.

10. The method of any one of claims 1 through 8, wherein the communication mode change command and the base value are received in a common message individualized for the receiving entity.

11. The method of any one of claims 1 through 10, further comprising ciphering outgoing device-to-device communications using the local device security key, and deciphering incoming device-to-device communications using the peer device security key.

12. An apparatus comprising at least one processor and at least one memory including computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus at least to perform:

receiving a communication mode change command requesting a mode change to device-to-device communications;

generating a local device security key based on a secret key and a base value, the local device security key being configured for use in device-to-device communications;

receiving a security key combination value; and

deconstructing the security key combination value using the local device security key to determine a peer device security key, the peer device security key being configured for use in device-to-device communications.

13. The apparatus of claim 12, wherein the apparatus caused to perform generating the local device security key based on the secret key and the base value includes being caused to perform generating the local device security key based on the secret key and the base value, wherein the base value is a random or pseudo-random number.

14. The apparatus of claim 12, wherein the apparatus is further caused to perform generating the base value.

15. The apparatus of claim 12, wherein the apparatus is further caused to perform:

generating the base value; and

causing sending of the base value to a key management network entity.

16. The apparatus of any one of claims 12 through 15, wherein the apparatus caused to perform receiving the security key combination value includes being caused to perform receiving the security key combination value from a mobility management entity.

17. The apparatus of claim 12, wherein the apparatus is further caused to perform:

generating the base value; and

causing sending of the base value to a key management network entity, the key management network entity being a mobility management entity.

18. The apparatus of any one of claims 11 through 17, wherein the apparatus caused to perform deconstructing the security key combination value includes being caused to perform implementing an exclusive-or operation on the security key combination value to determine the peer device security key.

19. The apparatus of any on of claims 11 through 18, wherein he apparatus caused to perform receiving the security key combination value includes being caused to perform receiving the security key combination value via a secure connection with the sending entity, the secure connection being a dedicated connection between the sending entity and a receiving entity.

20. The apparatus of any one of claims 11 through 19, wherein the apparatus is caused to receive the communication mode change command, the base value, and the security key combination value are received in a common message.

21. The apparatus of any one of claims 11 through 19, wherein the apparatus is caused to receive the communication mode change command and the base value are received in a common message individualized for the receiving entity.

22. The apparatus of any one of claims 11 through 21, wherein the apparatus is further caused to perform ciphering outgoing device-to-device communications using the local device security key, and deciphering incoming device-to-device communications using the peer device security key.

23. A apparatus comprising:

means for receiving a communication mode change command requesting a mode change to device-to-device communications;

means for generating a local device security key based on a secret key and a base value, the local device security key being configured for use in device-to-device communications;

means for receiving a security key combination value; and

means for deconstructing the security key combination value using the local device security key to determine a peer device security key, the peer device security key being configured for use in device-to-device communications.

24. The apparatus of 23, further comprising means for ciphering outgoing device-to-device communications using the local device security key, and means for deciphering incoming device-to-device communications using the peer device security key.

25. A method comprising:

generating a first security key for a first device based on a first secret key and a first base value, the first security key being configured for use in device-to-device communications from the first device;

generating a second security key for a second device based on a second secret key and a second base value, the second security key being configured for use in device-to-device communications from the second device;

combining the first security key with the second security key to generate a security key combination value; and

causing sending of the security key combination value.

26. The method of claim 25, wherein generating the first security key based on the first base value and generating the second security key based on the second base value includes generating the first security key based on the first base value and generating the second security key based on the second base value, wherein the first

base value is a first random or pseudo-random number associated with the first device and the second base value is a second random or pseudo-random number associated with the second device.

27. The method of claims 25 or 26, further comprising receiving the first base value from the first device, and receiving the second base value from the second device.

28. The method claims 25 or 26, further comprising generating the first base value and the second base value.

29. The method of any one of claims 25 through 28, wherein combining the first security key with the second security key includes combining the first security key with the second security key through an exclusive-or operation.

30. The method of any one of claims 25 through 29, wherein causing sending of the security key combination value includes causing sending of the security key combination value to the first device and the second device for deconstruction, or to an access point.

31. The method of any one of claims 25 through 29, further comprising:

receiving a request for the first security key and the second security key; and

causing sending of the first base value, the second base value, and the security key combination value to an access point.

32. An apparatus comprising at least one processor and at least one memory including computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus at least to perform:

generating a first security key for a first device based on a first secret key and a first base value, the first security key being configured for use in device-to-device communications from the first device;

generating a second security key for a second device based on a second secret key and a second base value, the second security key being configured for use in device-to-device communications from the second device;

combining the first security key with the second security key to generate a security key combination value; and

causing sending of the security key combination value.

33. The apparatus of claim 32, wherein the apparatus caused to perform generating the first security key based on the first base value and generating the second security key based on the second base value includes being caused to perform generating the first security key based on the first base value and generating the second security key based on the second base value, wherein the first base value is a first random or pseudo-random number associated with the first device and the second base value is a second random or pseudo-random number associated with the second device.

34. The apparatus of claims 32 or 33, wherein the apparatus is further caused to perform receiving the first base value from the first device, and receiving the second base value from the second device.

35. The apparatus claims 32 or 33, wherein the apparatus is further caused to perform generating the first base value and the second base value.

36. The apparatus of any one of claims 32 through 35, wherein the apparatus caused to perform combining the first security key with the second security key includes being caused to perform combining the first security key with the second security key through an exclusive-or operation.

37. The apparatus of any one of claims 32 through 36, wherein the apparatus caused to perform causing sending of the security key combination value includes being caused to perform causing sending of the security key combination value to the first device and the second device for deconstruction, or to an access point.

38. The apparatus of any one of claims 32 through 36, wherein the apparatus is further caused to perform:

receiving a request for the first security key and the second security key; and

causing sending of the first base value, the second base value, and the security key combination value to an access point.

39. An apparatus comprising:

means for generating a first security key for a first device based on a first secret key and a first base value, the first security key being configured for use in device-to-device communications from the first device;

means for generating a second security key for a second device based on a second secret key and a second base value, the second security key being configured for use in device-to-device communications from the second device;

means for combining the first security key with the second security key to generate a security key combination value; and

means for causing sending of the security key combination value.

40. The apparatus of 39, wherein the means for combining the first security key with the second security key includes means for combining the first security key with the second security key through an exclusive-or operation.

41. A method comprising:

generating a first base value for determining a first security key for use with device-to-device communications from a first device;

generating a second base value for determining a second security key for use with device-to-device communications from a second device;

causing sending of a communication mode change command to the first device and the second device with the first base value and the second base value;

causing sending of the first base value and the second base value to a key management network entity;

receiving a security key combination value from the key management network entity, the security key combination value being a combination of the first security key and the second security key; and

causing sending of the security key combination value to the first device and the second device.

42. The method of claim 41, wherein causing sending of the communication mode change command to the first device and the second device includes causing sending of a first communication mode change command with the first base value in an individualized message for the first device, and causing sending of a second communication mode change command with the second base value in an individualized message for the second device.

43. The method of claim 41 or 42, wherein causing sending of the security key combination value to the first device and the second device includes causing sending of the security key combination value via a dedicated and secure connection with the first

device, and causing sending of the security key combination value via a dedicated and secure connection with the second device.

44. An apparatus comprising at least one processor and at least one memory including computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus at least to perform:

generating a first base value for determining a first security key for use with device-to-device communications from a first device;

generating a second base value for determining a second security key for use with device-to-device communications from a second device;

causing sending of a communication mode change command to the first device and the second device with the first base value and the second base value;

causing sending of the first base value and the second base value to a key management network entity;

receiving a security key combination value from the key management network entity, the security key combination value being a combination of the first security key and the second security key; and

causing sending of the security key combination value to the first device and the second device.

45. The apparatus of claim 44, wherein the apparatus caused to perform causing sending of the communication mode change command to the first device and the second device includes being caused to perform causing sending of a first communication mode change command with the first base value in an individualized message for the first device, and causing sending of a second communication mode change command with the second base value in an individualized message for the second device.

46. The apparatus of claim 44 or 45, wherein the apparatus caused to perform causing sending of the security key combination value to the first device and the second device includes causing sending of the security key combination value via a dedicated and secure connection with the first device, and causing sending of the security key combination value via a dedicated and secure connection with the second device.

47. An apparatus comprising:

means for generating a first base value for determining a first security key for use with device-to-device communications from a first device;

means for generating a second base value for determining a second security key for use with device-to-device communications from a second device;

means for causing sending of a communication mode change command to the first device and the second device with the first base value and the second base value;

means for causing sending of the first base value and the second base value to a key management network entity;

means for receiving a security key combination value from the key management network entity, the security key combination value being a combination of the first security key and the second security key; and

means for causing sending of the security key combination value to the first device and the second device.

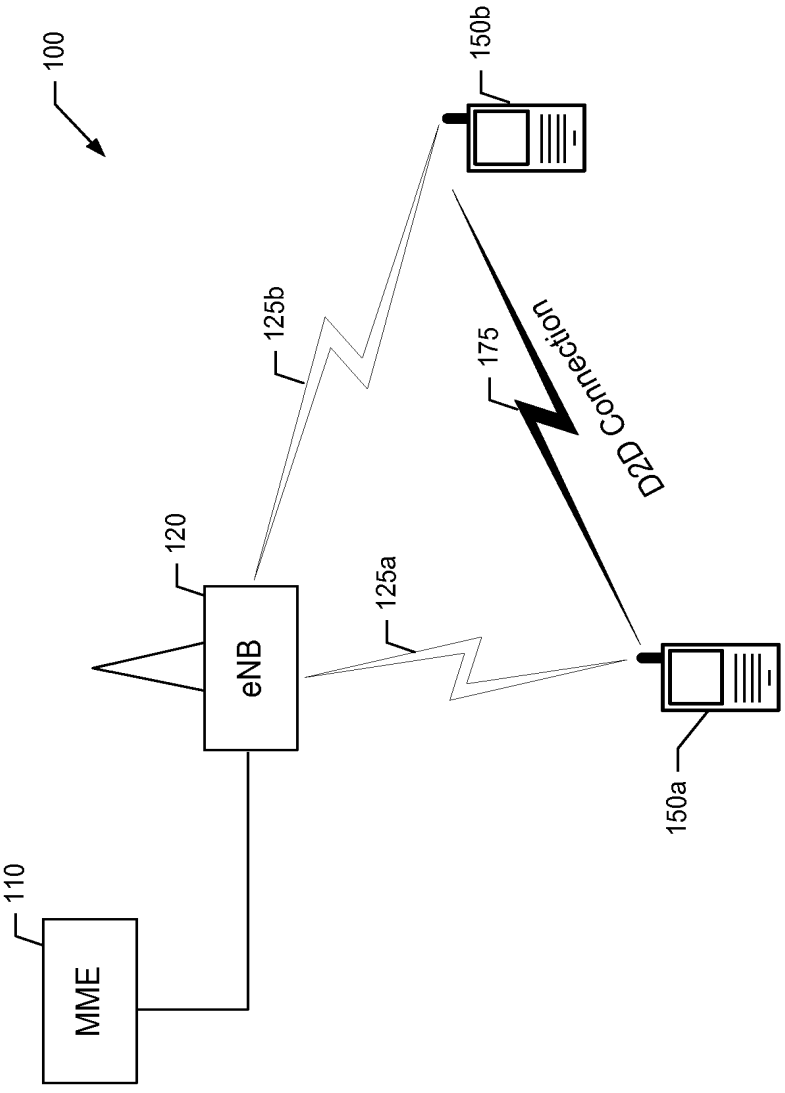


FIG. 1

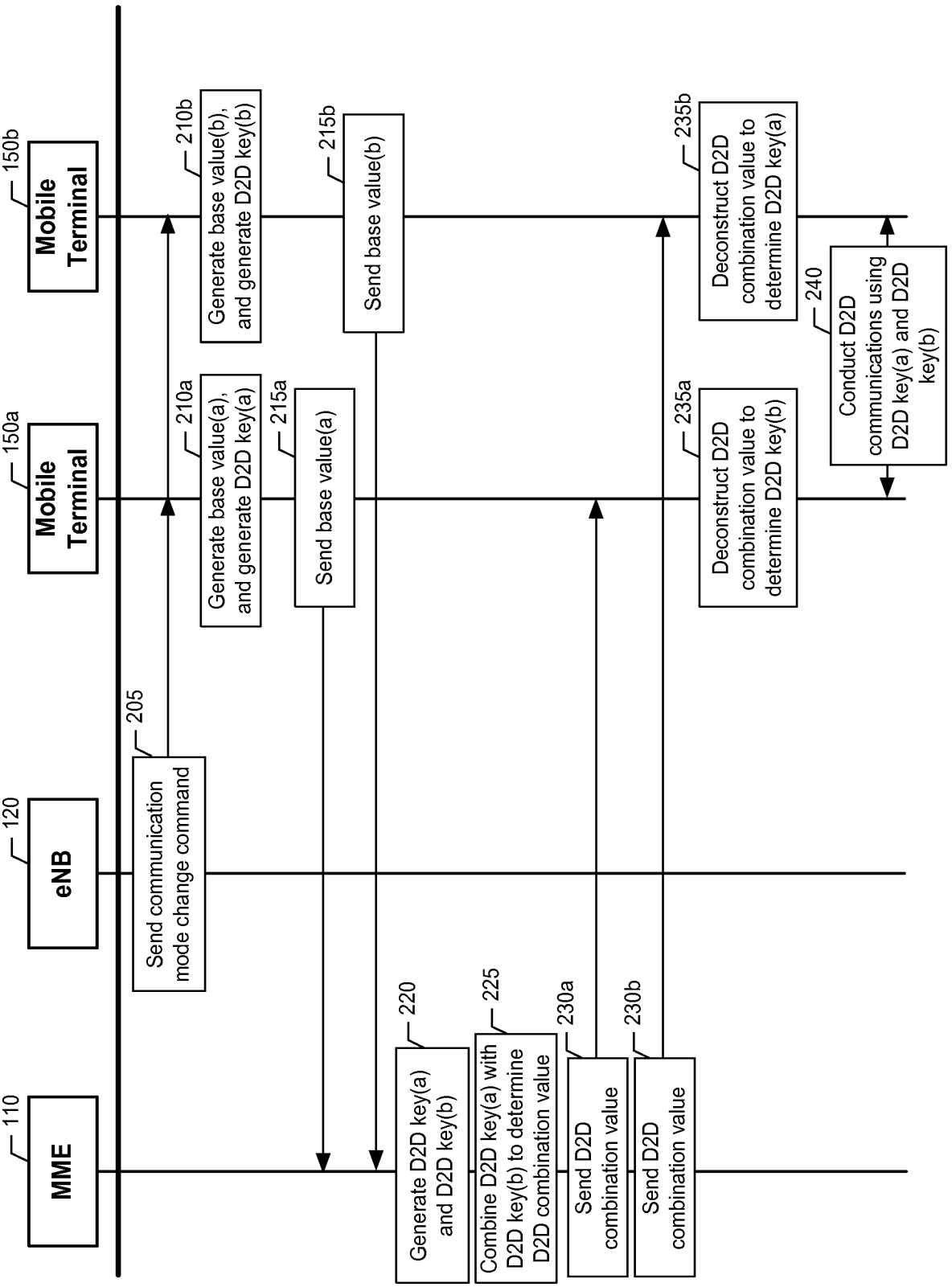

MME
110
eNB
120
Mobile Terminal
150a
Mobile Terminal
150b
205
Send communication mode change command
210a
Generate base value(a), and generate D2D key(a)
210b
Generate base value(b), and generate D2D key(b)
215a
Send base value(a)
215b
Send base value(b)
220
Generate D2D key(a) and D2D key(b)
225
Combine D2D key(a) with D2D key(b) to determine D2D combination value
230a
Send D2D combination value
230b
Send D2D combination value
235a
Deconstruct D2D combination value to determine D2D key(b)
235b
Deconstruct D2D combination value to determine D2D key(a)
240
Conduct D2D communications using D2D key(a) and D2D key(b)

FIG. 2

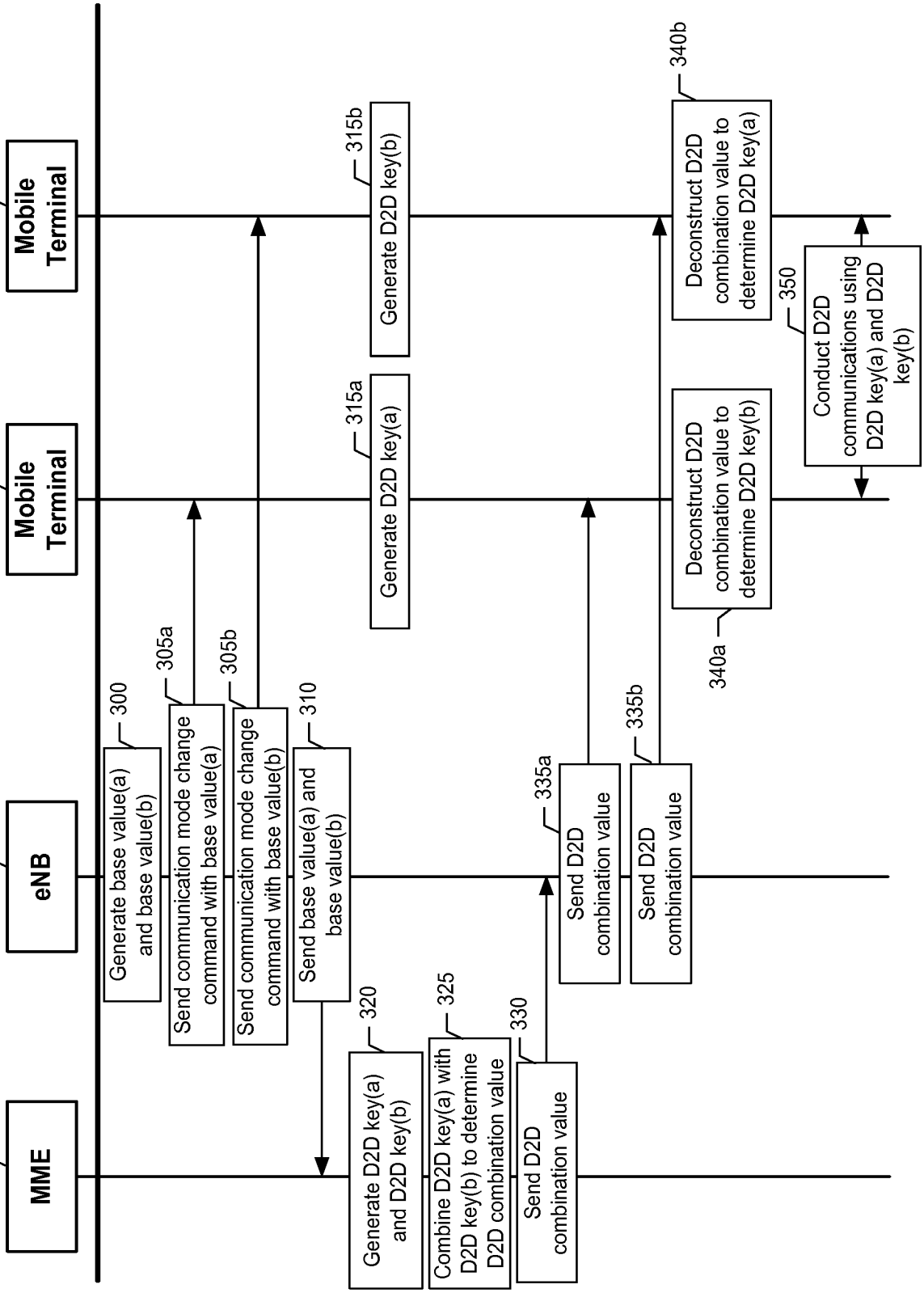

MME
110
eNB
120
Mobile Terminal
150a
Mobile Terminal
150b
Generate base value(a) and base value(b)
300
Send communication mode change command with base value(a)
305a
Send communication mode change command with base value(b)
305b
Send base value(a) and base value(b)
310
Generate D2D key(a) and D2D key(b)
320
Combine D2D key(a) with D2D key(b) to determine D2D combination value
325
Send D2D combination value
330
Generate D2D key(a)
315a
Generate D2D key(b)
315b
Send D2D combination value
335a
Send D2D combination value
335b
Deconstruct D2D combination value to determine D2D key(b)
340a
Deconstruct D2D combination value to determine D2D key(a)
340b
Conduct D2D communications using D2D key(a) and D2D key(b)
350

FIG. 3

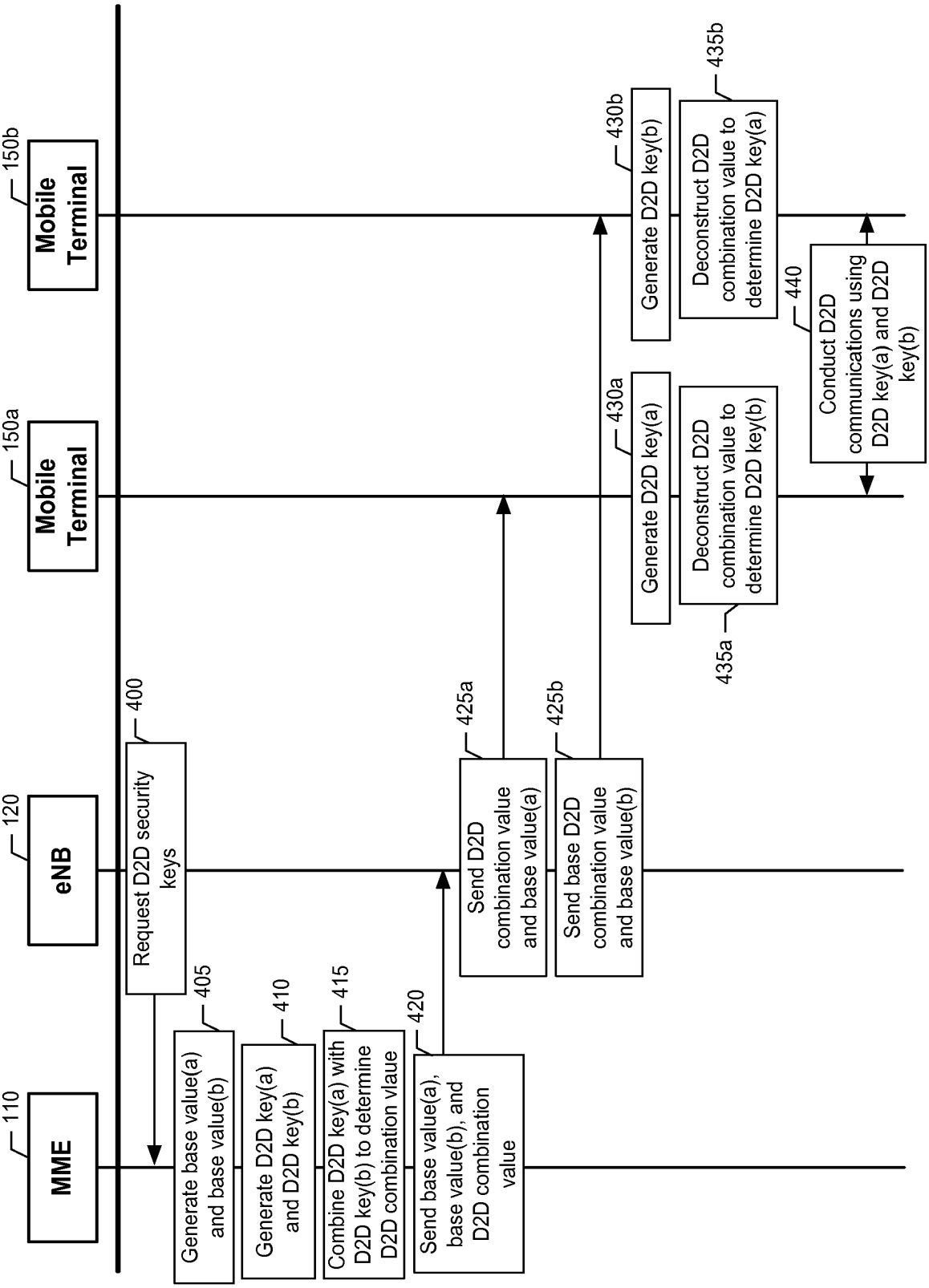

110
MME
120
eNB
150a
Mobile Terminal
150b
Mobile Terminal
400
Request D2D security keys
405
Generate base value(a) and base value(b)
410
Generate D2D key(a) and D2D key(b)
415
Combine D2D key(a) with D2D key(b) to determine D2D combination vlaue
420
Send base value(a), base value(b), and D2D combination value
425a
Send D2D combination value and base value(a)
425b
Send base D2D combination value and base value(b)
430a
Generate D2D key(a)
430b
Generate D2D key(b)
435a
Deconstruct D2D combination value to determine D2D key(b)
435b
Deconstruct D2D combination value to determine D2D key(a)
440
Conduct D2D communications using D2D key(a) and D2D key(b)

FIG. 4

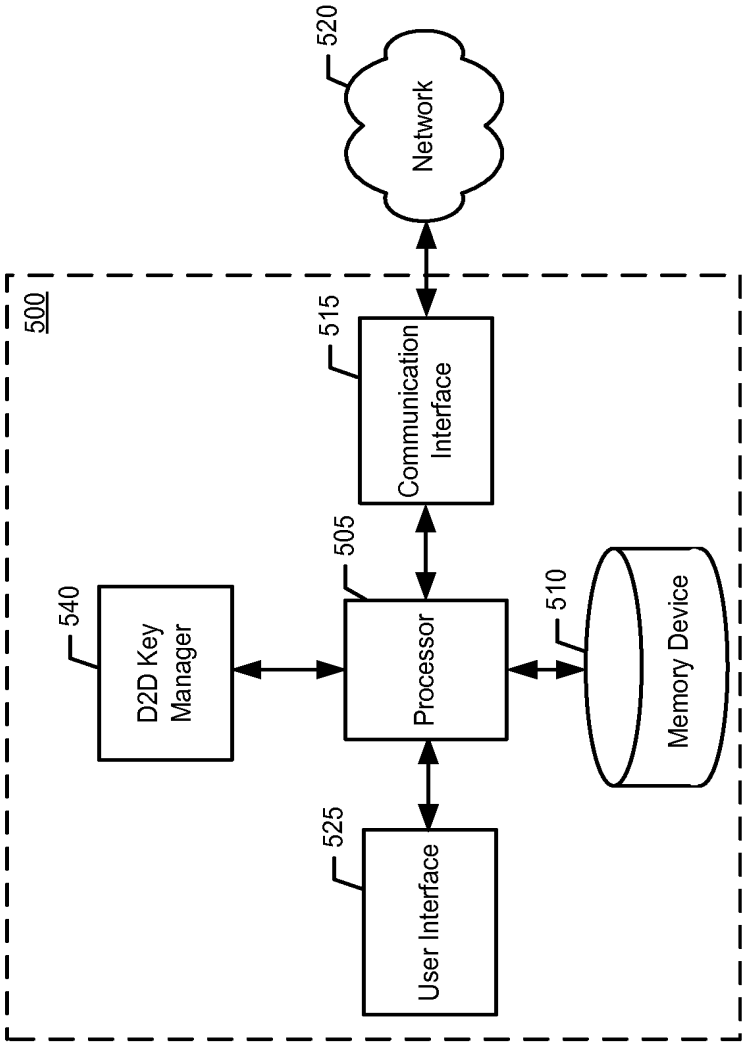

520
Network
500
515
Communication Interface
505
540
D2D Key Manager
Processor
510
Memory Device
525
User Interface

FIG. 5

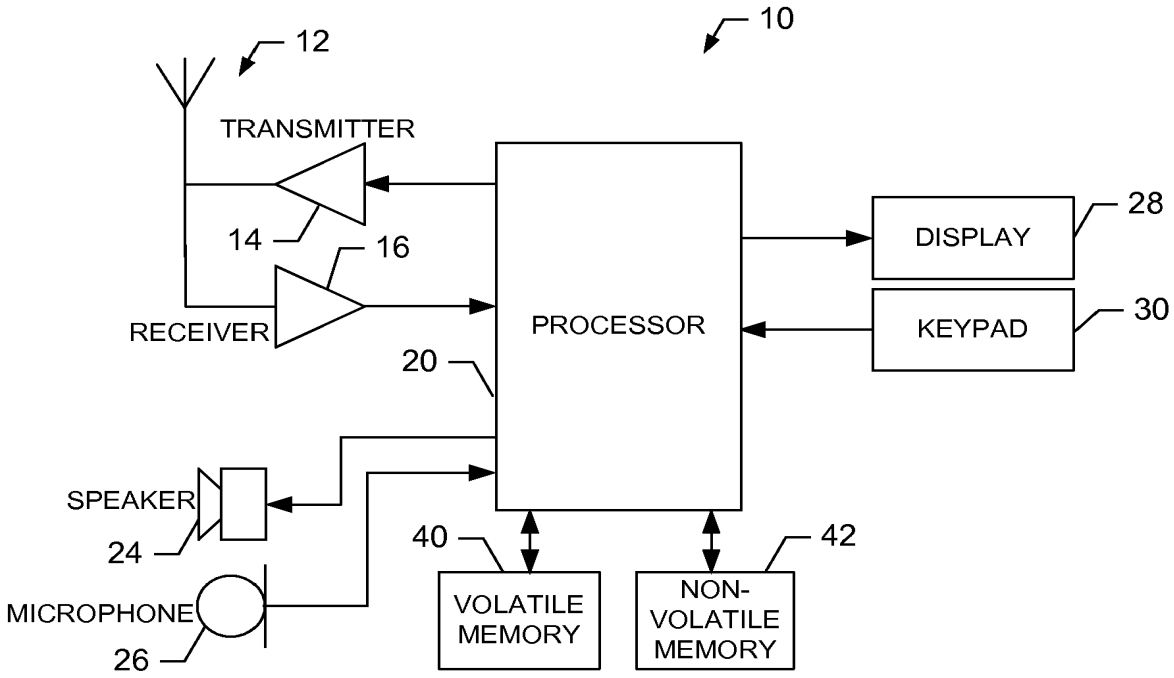

10
12
TRANSMITTER
14
16
RECEIVER
PROCESSOR
20
DISPLAY
28
KEYPAD
30
SPEAKER
24
MICROPHONE
26
40
VOLATILE MEMORY
42
NON-VOLATILE MEMORY

FIG. 6

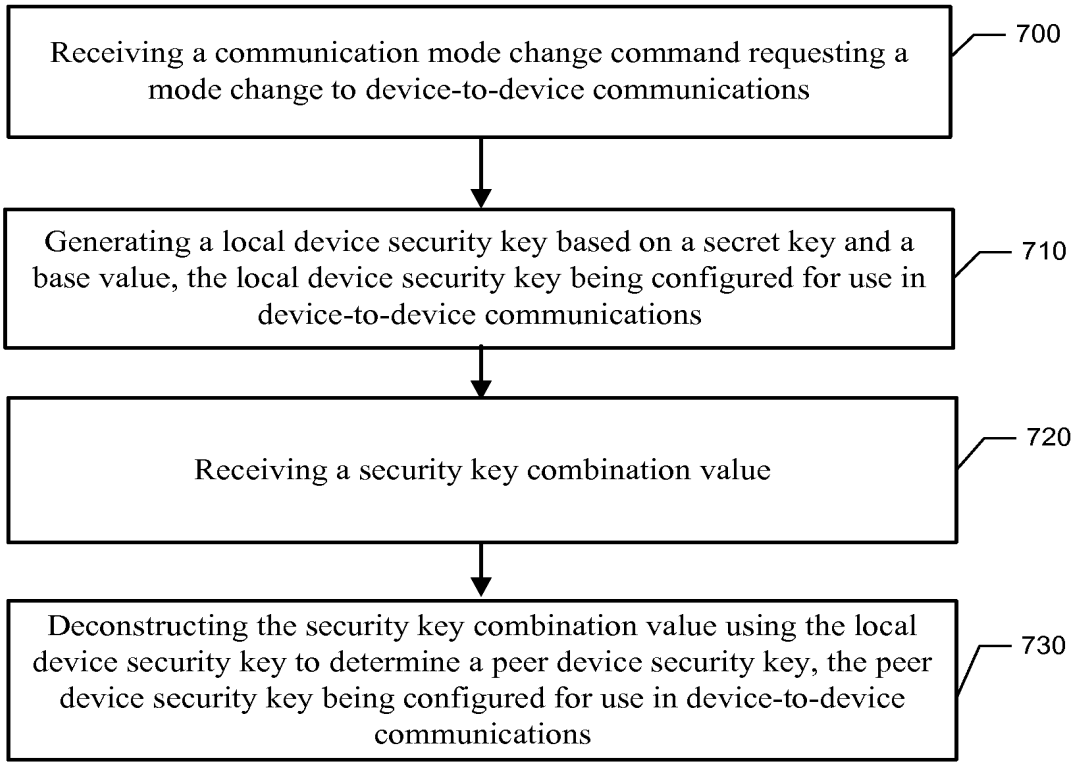

Receiving a communication mode change command requesting a mode change to device-to-device communications
700
Generating a local device security key based on a secret key and a base value, the local device security key being configured for use in device-to-device communications
710
Receiving a security key combination value
720
Deconstructing the security key combination value using the local device security key to determine a peer device security key, the peer device security key being configured for use in device-to-device communications
730

FIG. 7

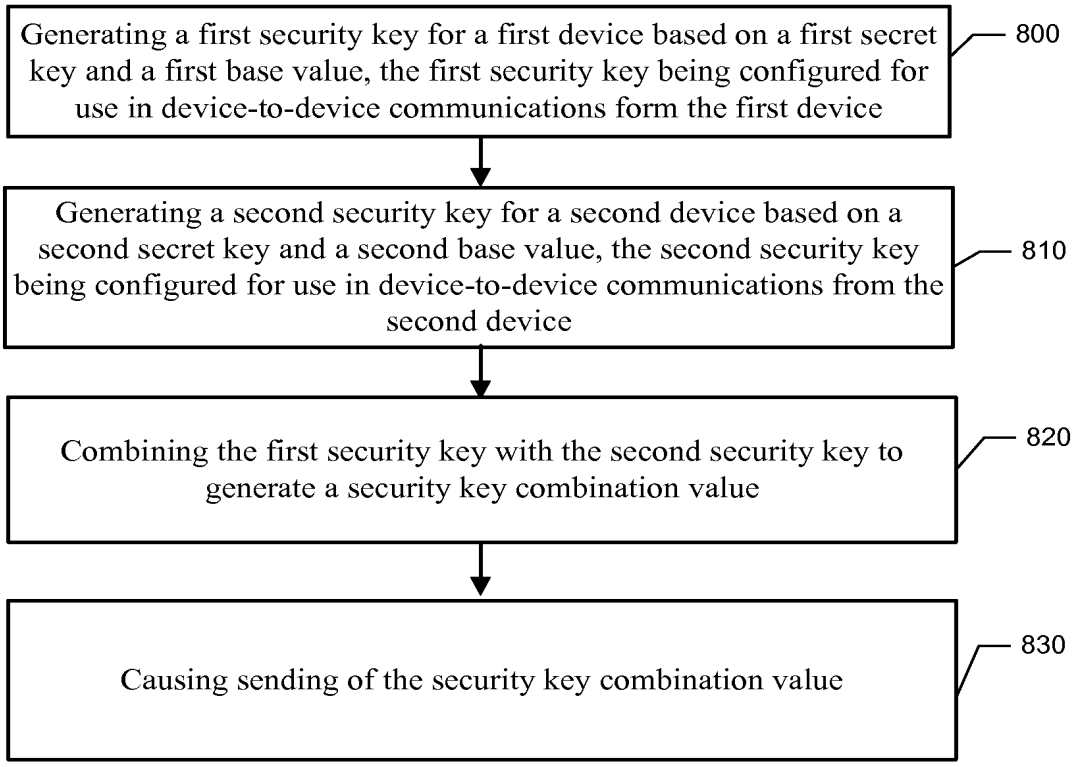

Generating a first security key for a first device based on a first secret key and a first base value, the first security key being configured for use in device-to-device communications form the first device
800
Generating a second security key for a second device based on a second secret key and a second base value, the second security key being configured for use in device-to-device communications from the second device
810
Combining the first security key with the second security key to generate a security key combination value
820
Causing sending of the security key combination value
830

FIG. 8

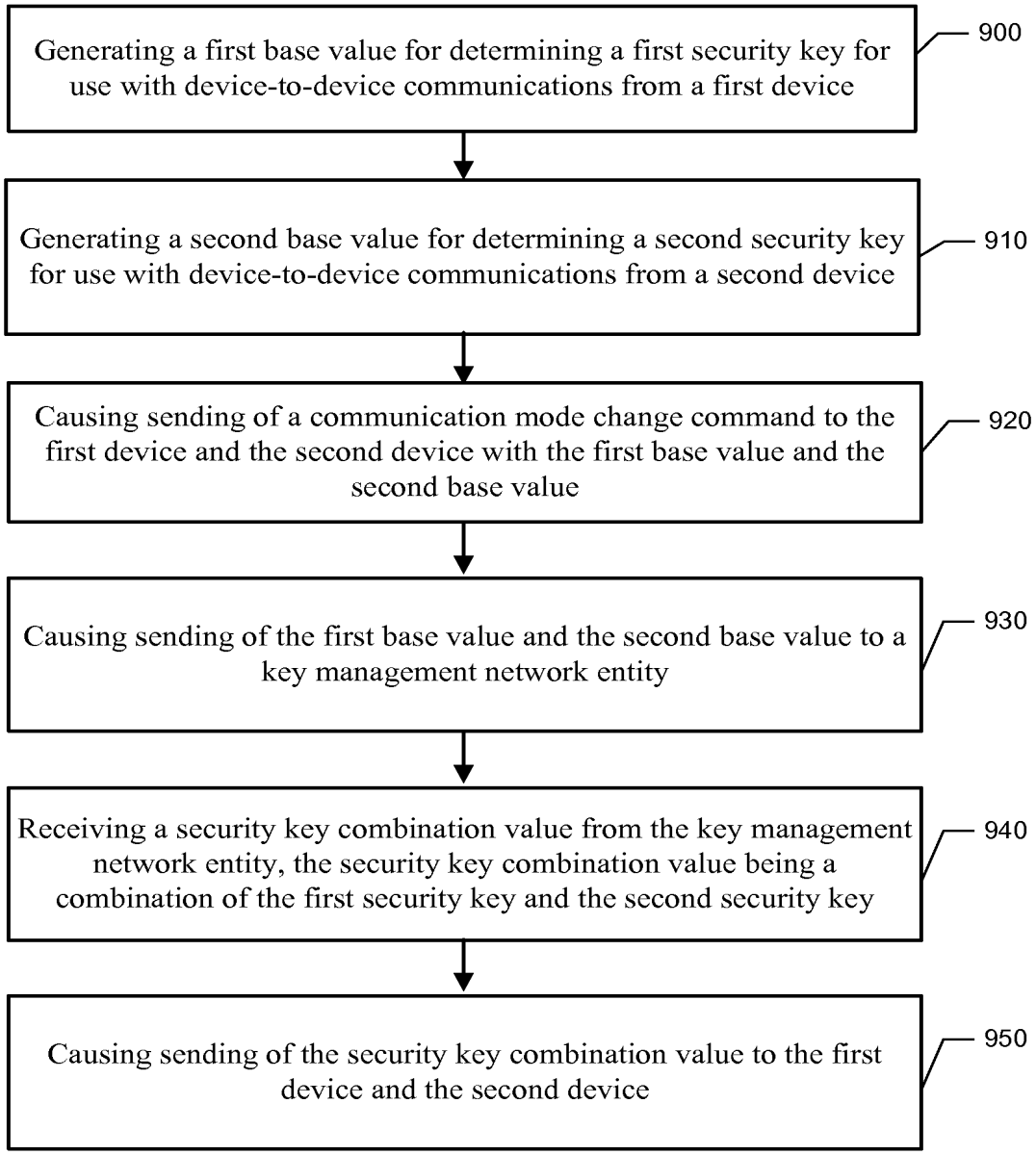

Generating a first base value for determining a first security key for use with device-to-device communications from a first device
900
Generating a second base value for determining a second security key for use with device-to-device communications from a second device
910
Causing sending of a communication mode change command to the first device and the second device with the first base value and the second base value
920
Causing sending of the first base value and the second base value to a key management network entity
930
Receiving a security key combination value from the key management network entity, the security key combination value being a combination of the first security key and the second security key
940
Causing sending of the security key combination value to the first device and the second device
950

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2010/051300

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI, XPAIP, XPESP, XPETSI, XPIEE, XPIETF, XPIOP, XPIPCOM, XPI3E, XPMISC, XPOAC, COMPENDEX, INSPEC, Google

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007253376 A1 (BONTA JEFFREY D et al.) 01 November 2007 (01.11.2007) [0002], [0004], [0013], [0016]-[0022], [0035], [0036], [0037], [0044], Figs. 1, 3	1-47
Y	US 2009320102 A1 (OU SHUKONG) 24 December 2009 (24.12.2009) [0015], [0021], [0027], [0028], [0029], Fig. 1, 3	1-24
Y	3GPP TS 33.401 v8.2.1 Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture,(Release 8), 19.12.2008 chapter 6, section 9.2.2, Annex A	1-47

☒ Further documents are listed in the continuation of Box C. ☒ 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 application or patent 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
23 December 2010 (23.12.2010)	28 December 2010 (28.12.2010)

Name and mailing address of the ISA/FI	Authorized officer
National Board of Patents and Registration of Finland P.O. Box 1160, FI-00101 HELSINKI, Finland	Jouko Berndtson
Facsimile No. +358 9 6939 5328	Telephone No. +358 9 6939 500

ERICSSON EXHIBIT 1002, Page 333

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	3GPP TR 33.821 v8.0.0 Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN; 3GPP System Architecture Evolution (SAE), (Release 8), 19.3.2009 section 7.4.3.1, section 7.4.13	1-47
A	US 2008095361 A1 (WIFVESSON MONICA et al.) 24 April 2008 (24.04.2008)	

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2007253376 A1	01/11/2007	RU 2008146960 A	10/06/2010
		MX 2008013772 A	15/04/2009
		WO 2007127637 A2	08/11/2007
		JP 2009535921T T	01/10/2009
		EP 2022282 A2	11/02/2009
		CA 2650050 A1	08/11/2007
		AU 2007242991 A1	08/11/2007
US 2009320102 A1	24/12/2009	None	
US 2008095361 A1	24/04/2008	WO 2008046863 A1	24/04/2008
		EP 2074741 A1	01/07/2009

International application No.
PCT/IB2010/051300

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)

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.
403638WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/EP2013/067904	29 August 2013 (29-08-2013)	6 September 2012 (06-09-2012)
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 5 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,**
   [ ] the text is approved as submitted by the applicant
   [X] the text has been established, according to Rule 38.2, 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

Box No. IV Text of the abstract (Continuation of item 5 of the first sheet)

A method is disclosed for establishing a device-to-device communication session between mobile devices (MDl, MD2) which are mutually connectable via a D2D communication channel (DDC) and individually connectable to a mobile network (MN), comprising:

- - preloading (120) an initiation key on each of the mobile devices (MD1, MD2), the initiation key being associated with a validity period; and on each of the mobile devices (MD1, MD2):
- - verifying (140) a validity of the initiation key based on a current time;
- - if the initiation key is deemed valid, generating (160) a session key using the initiation key by using the initiation key in performing (164, 166) a key agreement procedure between the mobile devices (MD 1, MD2) over the D2D communication channel (DDC), the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and
- - establishing (180) the D2D communication session over the D2D communication channel (DDC) based on the session key.

Figure 1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/067904

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/04 H04W74/08 H04W76/02
ADD.

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)
H04L H04W

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 practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2011/117677 A1 (NOKIA CORP [FI]; NOKIA INC [US]; HAKOLA SAMI-JUKKA [FI]; KOSKELA TIMO) 29 September 2011 (2011-09-29) page 7, line 8 - page 14, line 19 page 16, line 29 - page 20, line 8; claims 1-6,25-32,39-41; figures 1-6 -----	1-17
A	WO 2010/030515 A2 (QUALCOMM INC [US]; VANDERVEEN MICHAELA [US]; TSIRTSIS GEORGIOS [GB]; P) 18 March 2010 (2010-03-18) paragraph [0134] - paragraph [0137] paragraph [0155] - paragraph [0157]; figures 10-15 ----- -/--	1-17

[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 application or patent 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
25 September 2013	07/10/2013

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	Schwibinger, Hans

1

Form PCT/ISA/210 (second sheet) (April 2005)

ERICSSON EXHIBIT 1002, Page 339

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/067904

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GÃ BOR FODOR ET AL: "Design aspects of network assisted device-to-device communications", IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US, vol. 50, no. 3, 1 March 2012 (2012-03-01), pages 170-177, XP011429640, ISSN: 0163-6804, DOI: 10.1109/MCOM.2012.6163598 page 171, left-hand column, line 10 - page 172, right-hand column, line 29 page 174, left-hand column, line 1 - right-hand column, line 31; figures 1,2,4 -----	1-17
A	US 2007/253376 A1 (BONTA JEFFREY D [US] ET AL) 1 November 2007 (2007-11-01) paragraph [0017] - paragraph [0023] paragraph [0042] - paragraph [0047]; claims 1,12-14,17,19; figures 1,4,5 -----	1-17

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

ERICSSON EXHIBIT 1002, Page 340

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/067904

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2011117677 A1	29-09-2011	CN 102812688 A	05-12-2012
		EP 2550789 A1	30-01-2013
		US 2013013926 A1	10-01-2013
		WO 2011117677 A1	29-09-2011
WO 2010030515 A2	18-03-2010	CN 102124768 A	13-07-2011
		EP 2338296 A2	29-06-2011
		JP 2012502586 A	26-01-2012
		KR 20110067125 A	21-06-2011
		TW 201016043 A	16-04-2010
		US 2010069067 A1	18-03-2010
		US 2013227655 A1	29-08-2013
		WO 2010030515 A2	18-03-2010
US 2007253376 A1	01-11-2007	AU 2007242991 A1	08-11-2007
		BR PI0711079 A2	23-08-2011
		CA 2650050 A1	08-11-2007
		EP 2022282 A2	11-02-2009
		JP 4911480 B2	04-04-2012
		JP 2009535921 A	01-10-2009
		RU 2008146960 A	10-06-2010
		US 2007253376 A1	01-11-2007
		WO 2007127637 A2	08-11-2007

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wuyts, Koenraad Maria
Royal KPN N.V.
P.O. Box 95321
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)

	Date of mailing *(day/month/year)* 7 October 2013 (07-10-2013)
Applicant's or agent's file reference 403638WO	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/EP2013/067904	International filing date *(day/month/year)* 29 August 2013 (29-08-2013)
Applicant KONINKLIJKE KPN N.V.	

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 *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

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 any 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**

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. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

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 before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

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.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	ROTHENBüCHER, Anita Tel: +31 (0)70 340-9872

Form PCT/ISA/220 (July 2010)

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/EP2013/067904	29.08.2013	06.09.2012

International Patent Classification (IPC) or both national classification and IPC
INV. H04W12/04 H04W74/08 H04W76/02

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 and 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.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Schwibinger, Hans Telephone No. +31 70 340-1969

Form PCT/ISA/237 (Cover Sheet) (July 2009)

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, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ 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 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	1-17
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-17
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-17
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V.

1) Reference is made to the following documents:

D1 WO 2011/117677 A1 (NOKIA CORP [FI]; NOKIA INC [US]; HAKOLA SAMI-JUKKA [FI]; KOSKELA TIMO) 29 September 2011

D2 WO 2010/030515 A2 (QUALCOMM INC [US]; VANDERVEEN MICHAELA [US]; TSIRTSIS GEORGIOS [GB]; P) 18 March 2010

2) Clarity of the Independent Claims 1 and 16

The subject-matter of independent claim 1 comprises the technical feature in form of a method step:
'if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel,

the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches;'

The section printed in bold differs from the rest of the claim in that a different style of language is applied. Generally the claim has been drafted in a very technical style which the man skilled in the art knows from his text books. However, the section in bold applies a much more common style. Its teaching has been interpreted in the light of the description as described by the words

'if the validity of the initiation key has been verified by both mobile devices, the key agreement procedures will produce a session key;'

Since the skilled man cannot be sure whether his interpretation as given above is correct, the subject-matter of independent claims 1 and 16 is considered as not clear in violation of the requirements of Article 6 PCT.

3) Patentability of the Subject-Matter of Independent Claim 1

The publication D1, which is considered to represent the closest prior art, discloses in the terminology of independent claim 1 the following features (with relevant citations given in parenthesis):

Method for establishing a device-to-device communication session (: in the section BACKROUND D1 teaches the advantages of device-to-device communications, and the need to establish them safely) between mobile devices (:='mobile terminal 150a', 'mobile terminal 150b') which are mutually connectable via a D2D communication channel (:='D2D Connection') and individually connectable to a mobile network (:='n etwork connection 125a, 125b'), comprising:
- preloading an initiation key on each of the mobile devices (see figure 2, step 230a, 230b), the initiation key being associated with a validity period (: since figure 2 teaches the exchange of messages which lead to the key generation and distribution, the man skilled in the art interprets that the preloading of the initiation key has to be done within a limited validity period as otherwise the communication would naturally time out);
- establishing the D2D communication session over the D2D communication channel based on the session key (: see page 13, line 28 - 30).

The subject-matter of independent claim 1 differs from the teaching in D1 in two features:

i) - verifying a validity of the initiation key based on a current time;

il) - if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches;

Both these steps are performed on each mobile device.

Since these features are not part of the disclosure of D1, the subject-matter of independent claim 1 is considered novel (Article 33(2) PCT).

In the light of features i and ii, the technology disclosed in D1 shows the problem that playback attacks may still compromise the security of key distribution. To render such a playback attack impossible, the keys are distributed with information on their validity, which then gets checked by each mobile device.

As the technology disclosed by the subject-matter of independent claim 1 solves a problem, it is also considered as inventive (Article 33(2) EPC).

To complete this discussion it has to be said that the publication D2 teaches the use of certificates to enhance the security when distributing sensitive data (see in particular para 155 - 157). However D2's teaching will still need substantial adaptation

to be integrated into the teaching of D1, so that an argument that the subject-matter of independent claim 1 is based on a juxtaposition of D1 and D2's teaching would fail, as it is based on hindsight.

However, both D1 and D2 are certainly considered to be documents of utmost importance for the development of the technology disclosed in the application.

4) Dependent Claims 2 - 15

Since their parent claim, independent claim 1, has been considered as novel and inventive, also the subject-matter of dependent claims 2 - 15 is considered as novel and inventive (Article 33(2) and (3) PCT) since they do not introduce any negative features.

5) Independent Claim 16

The subject-matter of independent claim 16 is referring to a device which has been adapted to vitally contribute to the performance of the method defined in claim 1. Therefore analogous reasoning applies as given under item 3 and it is concluded that also the subject-matter of independent claim 16 is considered novel and inventive (Article 33(2) and (3) PCT).

6) Dependent Claim 17

Since the parent claim, independent claim 16, has been considered as novel and inventive, also the subject-matter of dependent claim 17 is considered as novel and inventive (Article 33(2) and (3) PCT) since it does not introduce any negative features.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Filer:	Timothy J. Meagher/Julie Kertyzak
Attorney Docket Number:	4965.1017-000

Filed as Large Entity

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
National Stage Fee	1631	1	280	280
Natl Stage Search Fee - Report provided	1642	1	480	480
National Stage Exam - all other cases	1633	1	720	720
Pages:				
Claims:				
Miscellaneous-Filing:				
Oath/Decl > 30 Mos From 371 commencement	1617	1	140	140
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1620**

Electronic Acknowledgement Receipt

EFS ID:	21622217
Application Number:	14424691
International Application Number:	PCT/EP2013/067904
Confirmation Number:	1653
Title of Invention:	Establishing A Device-To-Device Communication Session
First Named Inventor/Applicant Name:	Antonius Norp
Customer Number:	21005
Filer:	Timothy J. Meagher/Julie Kertyzak
Filer Authorized By:	Timothy J. Meagher
Attorney Docket Number:	4965.1017-000
Receipt Date:	27-FEB-2015
Filing Date:	
Time Stamp:	14:53:12
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	$1620
RAM confirmation Number	1253
Deposit Account	080380
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (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	49651017000Trans.pdf	124585 c070a90dafdc249c680998b43c96d81e0753e98b	no	3
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	496510170001stPgPCTApp.PDF	37969 662579262ca7bf3e40f7119fa425b14c68dcad8a	no	1
Warnings:					
Information:					
3	Application Data Sheet	49651017000ADS.PDF	1562785 c9677801cd3717ffc9db6c925376c28b490337d3	no	8
Warnings:					
Information:					
4		49651017000PrelimAmend.pdf	105354 b97f52182bca5aa53702b46fc7ce5d40fbd60e8d	yes	7

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Specification	2	2
Claims	3	6
Applicant Arguments/Remarks Made in an Amendment	7	7

Warnings:					
Information:					
5	Transmittal Letter	49651017000IDS.pdf	110710 1b21bfeeb9a4c35c6158c68ea9e2d08d74fbea31	no	3
Warnings:					
Information:					

6	Information Disclosure Statement (IDS) Form (SB08)	49651017000ListofRefs.pdf	116412 af097814a444d1dfbe991d5d8f1c6939803067f6	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
7	Foreign Reference	49651017000For1.pdf	2743547 a78753c1dee8c294840d2c2281df22eae7a79599	no	66
Warnings:					
Information:					
8	Foreign Reference	49651017000For2.pdf	1941666 77ae495c51dd621acc0b3f93d0940e695bba8e06	no	44
Warnings:					
Information:					
9	Non Patent Literature	49651017000NPL1.pdf	1502275 332b3a738e635b84e3d9cdc3e842ab9f02b54be2	no	8
Warnings:					
Information:					
10	Non Patent Literature	49651017000NPL2.pdf	392969 8db5fdaa7260be2400a4dfa4916721b72081c315	no	11
Warnings:					
Information:					
11	Fee Worksheet (SB06)	fee-info.pdf	37010 ef25c91dda8db511d8e48ca19e68fd6da8092fbe	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	8675282		

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.

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

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 4965.1017-000 U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
INTERNATIONAL APPLICATION NO. PCT/EP2013/067904	INTERNATIONAL FILING DATE August 29, 2013	PRIORITY DATE CLAIMED September 6, 2012

TITLE OF INVENTION

Establishing A Device-To-Device Communication Session

FIRST NAMED INVENTOR Antonius Norp

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required).
2. ☐ A copy of the International Application (35 U.S.C. 371(c)(2), is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)).
3. ☐ An English language translation of the International Application (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
4. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))
   a. ☐ is attached hereto.
   b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv).

Items 5 to 8 below concern amendments made in the international phase.

PCT Article 19 and 34 amendments

5. ☐ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)).
6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)).
7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)).

Cancellation of amendments made in the international phase

8a. ☐ Do not enter the amendment made in the international phase under PCT Article 19.

8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34.

NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s).

The following items 9 to 17 concern a document(s) or information included.

9. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
10. ☒ A preliminary amendment.
11. ☒ An Application Data Sheet under 37 CFR 1.76.
12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).
13. ☐ A power of attorney and/or change of address letter.
14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821-1.825.
15. ☐ Assignment papers (*cover sheet and document(s)*). Name of Assignee: [_____]
16. ☐ 37 CFR 3.73(c) Statement (*when there is an Assignee*).

U.S. APPLICATION NO. (if known - see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
	PCT/EP2013/067904	4965.1017-000

17. ☒ Other items or information:
1st page of PCT application

The following fees have been submitted		CALCULATIONS	PTO USE ONLY
18. ☒ Basic national fee (37 CFR 1.492(a))	**$280**	$280	
19. ☒ 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	**$720**	$720	
20. ☒ 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	**$120**		
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	**$480**		
All other situations	**$600**	$480	
TOTAL OF 18, 19, and 20 =		$1480	

☐ 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)).
Fee for each additional 50 sheets of paper or fraction thereof ……**$400**

Total Sheets	Extra sheets	Number of each additional 50 or fraction thereof (round **up** to a whole number)	RATE	
32 - 100 =	/50 =		**x $400**	$

Surcharge of **$140** 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)). $140

CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE		
Total claims	17	- 20 =	0	x **$80**	$	
Independent claims	2	- 3 =	0	x **$420**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)				+ **$780**	$	
				TOTAL OF ABOVE CALCULATIONS =	$1620	

☐ Applicant claims small entity status. See 37 CFR 1.27. Fees above are reduced by 50%. $

☐ Applicant claims micro entity status. See 37 CFR 1.29. Fees above are reduced by 75%. $

SUBTOTAL = $1620

Processing fee of **$140** for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)). + $

TOTAL NATIONAL FEE = $1620

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 if filed by mail. **$0** if electronically filed. + $

TOTAL FEES ENCLOSED = $1620

Amount to be refunded:	$
Amount to be charged:	$

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
	PCT/EP2013/067904	4965.1017-000

a. ☐ A check in the amount of $[ ] to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 08-0380 in the amount of $1620 to cover the above fees.

c. ☒ The Director is hereby authorized to charge any deficiency or credit any overpayment in the fees that may be due in this matter to Deposit Account No. 08-0380.

d. ☐ The Director is hereby authorized to charge the basic filing fee to Deposit Account No. 08-0380.

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.

Correspondence Address

☒ The address associated with Customer Number: **021005** or ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone			
Email					

Signature	/Timothy J. Meagher, Reg. No. 39,302/	Date	2/27/2015
Name (Print/Type)	Timothy J. Meagher	Registration No. (Attorney/Agent)	39,302

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 March 2014 (13.03.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/037277 A1

(51) International Patent Classification:
H04W 12/04 (2009.01) *H04W 76/02* (2009.01)
H04W 74/08 (2009.01)

(21) International Application Number:
PCT/EP2013/067904

(22) International Filing Date:
29 August 2013 (29.08.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12183256.2 6 September 2012 (06.09.2012) EP

(71) Applicants: **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: **NORP, Antonius**; Cornelis Jolstraat 83, NL-2584 EN The Hague (NL). **FRANSEN, Frank**; Brilweg 21, NL-9801 GC Zuidhorn (NL). **DE KIEVIT, Sander**; Ravenhorst 61, NL-2317 AG Leiden (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, BN, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, 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: ESTABLISHING A DEVICE-TO-DEVICE COMMUNICATION SESSION

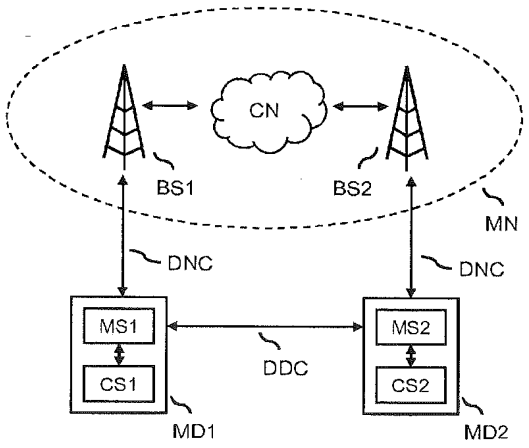


Fig. 1

(57) Abstract: A method is disclosed for establishing a device-to-device communication session between mobile devices (MD1, MD2) which are mutually connectable via a D2D communication channel (DDC) and individually connectable to a mobile network (MN), comprising: • - preloading (120) an initiation key on each of the mobile devices (MD1, MD2), the initiation key being associated with a validity period; and on each of the mobile devices (MD1, MD2): • - verifying (140) a validity of the initiation key based on a current time; • - if the initiation key is deemed valid, generating (160) a session key using the initiation key by using the initiation key in performing (164, 166) a key agreement procedure between the mobile devices (MD1, MD2) over the D2D communication channel (DDC), the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and • - establishing (180) the D2D communication session over the D2D communication channel (DDC) based on the session key.

WO 2014/037277 A1

TJM/jk
February 27, 2015

IN THE UNITED STATES RECEIVING OFFICE (RO/US)
Designated/Elected Office (DO/EO/US)

U.S. National Stage of International Application No.: PCT/EP2013/067904

International Filing Date: August, 29 2013

Earliest Priority Date: September 6, 2012

Inventor(s): Antonius Norp, Frank Fransen and Sander De Kievit

Title: Establishing A Device-To-Device Communication Session

Attorney's Docket No.: 4965.1017-000

DATE:_____

EXPRESS MAIL LABEL NO._____

PRELIMINARY AMENDMENT

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

Commissioner:

Please amend the application as follows:

Amendments to the Specification

Please add the following "Related Applications" paragraph after the Title at page 1, line 1:

This application is the U.S. National Stage of International Application No. PCT/EP2013/067904, filed August 29, 2013, which designates the U.S., published in English, and claims priority under 35 U.S.C. §§ 119 or 365(c) to European Application No. 12183256.2, filed September 6, 2012.

Amendments to the Claims

Please cancel claims 1-17. Please add claims 18-34. The Claim Listing below will replace all prior versions of the claims in the application:

Claim Listing

1. - 17. (Cancelled)

18. (New) Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:

preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and on each of the mobile devices:

verifying a validity of the initiation key based on a current time;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by each of the mobile devices matches; and

establishing the D2D communication session over the D2D communication channel based on the session key.

19. (New) Method according to claim 18, wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network.

20. (New) Method according to claim 18, wherein the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device.

21. (New) Method according to claim 20, wherein the secure storage area is provided by a trusted computing subsystem of each respective mobile device.

22. (New) Method according to claim 21, wherein at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem.

23. (New) Method according to claim 18, further comprising:

preloading a set of initiation keys on each of the mobile devices, the set of initiation keys key being associated with a respective set of validity periods; and

performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.

24. (New) Method according to claim 23, further comprising:

preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys; and

performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.

25. (New) Method according to claim 23, further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session.

26. (New) Method according to claim 23, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods.

27. (New) Method according to claim 18, wherein the initiation key is associated with a virtual network identity, and wherein the verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel.

28. (New) Method according to claim 18, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and wherein the verifying the validity of the initiation key is further based on the usage count.

29. (New) Method according to claim 28, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session.

30. (New) Method according to claim 18, further comprising requesting a further initiation key via the mobile network if i) no initiation key is deemed valid, or ii) the key agreement procedure fails in providing the session key.

31. (New) Method according to claim 18, wherein the key agreement procedure comprises:

a three-pass authentication procedure; or

a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.

32. (New) Control software comprising instructions for, upon execution of the control software on a mobile device, causing the mobile device to establish the D2D communication session according to the method of claim 18.

33. (New) Mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:

a storage area for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and

a computing subsystem for:

verifying a validity of the initiation key based on a current time;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device and the further mobile device matches; and

a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

34. (New) Mobile network arranged for preloading an initiation key on a mobile device according to claim 33 when the mobile device is connected to the mobile network, the initiation key being associated with a validity period.

REMARKS

Original Claims 1-17 have been cancelled and represented as claims 18-34 without multiple dependencies and without parenthetical abbreviations and numerals. A "Related Applications" paragraph has been added.

Information Disclosure Statement

An Information Disclosure Statement (IDS) is being filed concurrently herewith. Entry of the IDS is respectfully requested.

CONCLUSION

Entry of the Preliminary Amendment is respectfully requested. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned at (978) 341-0036.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By /Timothy J. Meagher, Reg. No. 39,302/
Timothy J. Meagher
Registration No. 39,302
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 2/27/2015

TJM/jk
February 27, 2015

IN THE UNITED STATES RECEIVING OFFICE (RO/US)
Designated/Elected Office (DO/EO/US)

U.S. National Stage of International Application No.:	PCT/EP2013/067904
International Filing Date:	August, 29 2013
Earliest Priority Date:	September 6, 2012
Inventor(s):	Antonius Norp, Frank Fransen and Sander De Kievit
Title:	Establishing A Device-To-Device Communication Session
Attorney's Docket No.:	4965.1017-000

DATE:_____

EXPRESS MAIL LABEL NO._____

TRANSMITTAL LETTER FOR
INFORMATION DISCLOSURE STATEMENT

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

Commissioner:

This Information Disclosure Statement is submitted:

☒ under 37 CFR 1.97(b), or
(Within any one of the following time periods: three months of filing national application (other than a CPA) or date of entry of the national stage in an international application; or before the mailing date of a first office action on the merits; or before the mailing of a first office action after the filing of a Request for Continued Examination).

☐ under 37 CFR 1.97(c) together with either:
- ☐ a Statement under 37 CFR 1.97(e), as checked below, or
- ☐ a $180.00 fee under 37 CFR 1.17(p), or
(After the 37 CFR 1.97(b) time period, but before any of a final action, notice of allowance, or an action that closes prosecution, whichever occurs first)

☐ under 37 CFR 1.97(d) together with:
- ☐ a Statement under 37 CFR 1.97(e), as checked below, and
- ☐ a $180.00 fee under 37 CFR 1.17(p), or
(Filed after final action, notice of allowance, whichever occurs first, or if prosecution otherwise closes, but on or before payment of the issue fee)

☐ under 37 CFR 1.97(i):
Applicant requests that the IDS and cited reference(s) be placed in the application file.
(Filed after payment of issue fee)

No aspect of this submission constitutes a disclaimer of claim scope.

Statement Under 37 CFR 1.97(e)

☐ Each item of information contained in this 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 this Information Disclosure Statement; or

☐ No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, 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 this Information Disclosure Statement.

Statement Under 37 CFR 1.704(d) (Patent Term Adjustment)
Applies to original applications (other than design) filed on or after May 29, 2000

☐ (1) A paper containing only an information disclosure statement in compliance with §§ 1.97 and 1.98 will not be considered a failure to engage in reasonable efforts to conclude prosecution (processing or examination) of the application under paragraphs (c)(6), (c)(8), (c)(9), or (c)(10) of this section if it is accompanied by a statement that each item of information contained in the information disclosure statement:

- ☐ (i) Was first cited in any communication from a patent office in a counterpart foreign or international application or from the Office, and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the information disclosure statement; or
- ☐ (ii) Is a communication that was issued by a patent office in a counterpart foreign or international application or by the Office, and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the information disclosure statement.

☒ Enclosed herewith is a Listing of References. Copies of the cited references are enclosed except as indicated below or in the attached Listing of References.

☐ Copies of the cited references submitted with an Information Disclosure Statement in prior application, U.S. Application No. [ ], to which priority under 35 U.S.C. 120 is claimed, are not required under 37 CFR 1.98(d)(1) and (2) and are thus not provided.

☒ The listed references were cited in the enclosed Search Report in counterpart application PCT/EP2013/067904, which is listed in the attached Listing of References.

☐ The "concise explanation" requirement (non-English references) for reference(s) [ ] under 37 CFR 1.98(a)(3) is satisfied by:

- ☐ the explanation provided on the attached sheet.
- ☐ the explanation provided in the Specification.
- ☐ submission of the enclosed International Search Report.
- ☐ submission of the enclosed English-language version of a foreign Search Report and/or foreign Office Action.
- ☐ the enclosed English language abstract.

Method of payment:

☐ A check for the fee noted above is enclosed, or the fee has been included in the check with the accompanying Reply.

☐ Please charge Deposit Account 08-0380 in the amount of $[ ].

☒ Please charge any deficiency in fees and credit any overpayment to Deposit Account 08-0380.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By /Timothy J. Meagher, Reg. No. 39,302/
Timothy J. Meagher
Registration No.: 39,302
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 2/27/2015

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 14/424,691	Filing Date 02/27/2015	☐ 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	02/27/2015	(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))	* 17	Minus	** 20	= 0	X $80 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 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
/PATRICIA WARNER/

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.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

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.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Antonius		Norp	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	The Hague	Country of Residence [i]	NL

Mailing Address of Inventor:

Address 1	Cornelis Jolstraat 83		
Address 2			
City	The Hague	State/Province	
Postal Code	NL-2584	Country [i]	NL

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Frank		Fransen	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Zuidhorn	Country of Residence [i]	NL

Mailing Address of Inventor:

Address 1	Brilweg 21		
Address 2			
City	Zuidhorn	State/Province	
Postal Code	NL-9801	Country [i]	NL

Inventor 3 Remove

Legal Name

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Sander		De Kievit	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Leiden	Country of Residence [i]	NL

Mailing Address of Inventor:

Address 1	Ravenhorst 61		
Address 2			
City	Leiden	**State/Province**	
Postal Code	NL-2317	**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.**

Customer Number	021005		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Establishing A Device-To-Device Communication Session		
Attorney Docket Number	4965.1017-000	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	5	**Suggested Figure for Publication (if any)**	1

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

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). Either enter 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	021005		

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.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	a 371 of international	PCT/EP2013/067904	2013-08-29

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. 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(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[j] (if applicable)
12183256.2	EP	2012-09-06	

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.
In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

(●) Assignee	( ) Legal Representative under 35 U.S.C. 117	( ) Joint Inventor
( ) Person to whom the inventor is obligated to assign.	( ) Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. [X]

Organization Name	Koninklijke KPN N.V.

Mailing Address Information For Applicant:

Address 1	P.O. Box 95321		
Address 2			
City	The Hague	**State/Province**	
Country	NL	Postal Code	2509 CH
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Applicant 2

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

(●) Assignee	( ) Legal Representative under 35 U.S.C. 117	( ) Joint Inventor
( ) Person to whom the inventor is obligated to assign.	( ) Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

If the Applicant is an Organization check here. ☒			
Organization Name	Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO		
Mailing Address Information For Applicant:			
Address 1	Anna van Buerenplein 1		
Address 2			
City	Den Haag	**State/Province**	
Country i	NL	Postal Code	2595 DA
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4965.1017-000
	Application Number	
Title of Invention	Establishing A Device-To-Device Communication Session	

Signature:

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

Signature	/Timothy J. Meagher, Reg. No. 39302/			Date (YYYY-MM-DD)	2015-02-27
First Name	Timothy J.	Last Name	Meagher	Registration Number	39302

Additional Signature may be generated within this form by selecting the Add button.

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 C o o p eration 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.