(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 October 2009 (15.10.2009)

PCT

(10) International Publication Number
WO 2009/124889 A1

(51) International Patent Classification:
H04N 7/16 (2006.01)

(21) International Application Number:
PCT/EP2009/054019

(22) International Filing Date:
3 April 2009 (03.04.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08290363.4 11 April 2008 (11.04.2008) EP

(71) Applicant *(for all designated States except US)*: **GEMALTO SA** [FR/FR]; Intellectual Property Dpt, 6 rue de la Verrerie, F-92190 Meudon (FR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SEIF, Jacques** [FR/FR]; c/o GEMALTO SA, Intellectual Property Dpt, 6 rue de la Verrerie, F-92197 Meudon Cedex (FR).

(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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, 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))*

WO 2009/124889 A1

(54) Title: METHOD FOR PROTECTION OF KEYS EXCHANGED BETWEEN A SMARTCARD AND A TERMINAL

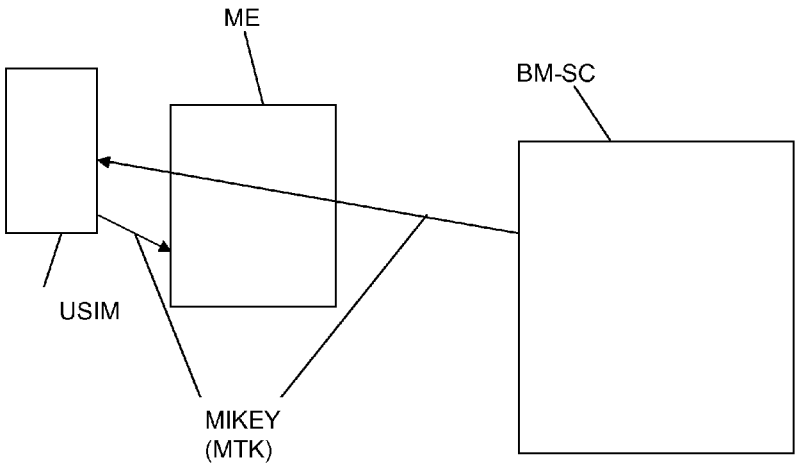

FIG.1

(57) Abstract: The present invention relates to a method for the protection of keys sent from a secure token (USIM) to a terminal (ME), said keys being traffic keys (MTK) used to decrypt a portion of content received from a content delivery center (BM-SC), said traffic keys being sent from said content delivery center (BM-SC) to the secure token (USIM) via a terminal (ME) using the MIKEY protocol defined by IETF RFC 3830. The method further comprises the steps of (a) - decrypting in the secure token encrypted traffic keys received from content delivery center thereby producing traffic keys, and decryption by the terminal (ME) of the content received from the content delivery center (BM-SC) by using said traffic keys, characterized in that said method further comprises the step of (b) - encrypting in the secure token, using the MIKEY protocol defined by IETF RFC 4738, said traffic keys, and decryption by the terminal of said IETF RFC 3830-protocol-encrypted traffic keys.

METHOD FOR PROTECTION OF KEYS EXCHANGED BETWEEN A SMARTCARD AND A TERMINAL

TECHNICAL FIELD

This invention relates to a method for protecting keys exchanged between a smartcard and a terminal. The invention relates to a method for a service provider to ensure that a subscriber cannot conspire to circumvent the security solution to distribute so-called traffic service keys to malicious users who will get free access to a service for which a subscription and/or a payment is required.

BACKGROUND

It is typical for mobile TV services systems to encrypt the distributed content to be able to protect and charge the access to this content. The content, e.g. a TV program, can be distributed in broadcast, multicast or unicast modes or any combination. In parallel to the encrypted content distribution, it is also common in such systems to distribute traffic keys to valid subscribers in order to provide them access to the service content. A traffic key is used for the descrambling/decryption of a portion of the distributed content and typically changes after a short period. The service provider needs obviously to also protect these traffic keys to valid subscribers. Otherwise, an attacker can simply eavesdrop on traffic key distribution and get access to the encrypted and protected content.

Although entities such as service providers and subscribers are used here in association with key distribution functions, those skilled in the art would readily appreciate that these entities do not by themselves carry out key distribution but equipment associated therewith that does. For the service providers, the equipment involved includes a server (e.g. BM-SC). For the subscriber, the equipment involved includes an authentication token, such as a subscriber identity module (SIM or USIM), supported in a mobile equipment or terminal (hereinafter “ME”).

For performances and technical limitations reasons, it is very difficult to the service provider to send traffic keys to millions of subscribers individually as these traffic keys are frequently changed for security reasons (e.g. they are changed each 30 seconds to prevent an attacker who get one traffic key to get access to the service for a long time). Therefore, in such systems, usually the traffic key distribution is usually protected by a service key (e.g. MSK key in MBMS systems or SEK/PEK in OMA BCAST systems) to protect and simplify the traffic key delivery. The service key is less frequently updated than the traffic key (e.g. one per week or month). Therefore, it is possible to send individually such key to the subscriber. But the service key is a key asset for the service provider as compromising this key can result in large scale free access to the service for long periods of time. Therefore, the service provider usually deliver and securely store the service key to the authentication token such as the USIM smartcard. The authentication token, which is a tamper resistant hardware device protects the storage of the service key and prevent any access to this key from outside the authentication token. The service key in the authentication token is then used by the server and the authentication token to secure (e.g. by encryption and integrity protection) the delivery of the traffic keys to the authentication token which then send them to the ME. The ME, which receives the traffic key from the authentication token and the encrypted broadcasted content, decrypt the content and render it to the user.

In order to circumvent the security solution, a valid subscriber can spy on the interface between the authentication token and the ME. This raises a serious fraud problem for the service provider. An attacker having a legitimate authentication token can save the traffic keys exchanged between the authentication token and the ME and then distribute these keys (e.g. over the internet) to malicious subscribers to get free access to the service. Furthermore, some content are sold to be viewed once. The attacker may use the saved keys to replay the content indefinitely.

It is thus desirable for the service provider to be able to protect the traffic key exchange between the authentication token and the ME. It is also desirable for the service provider to minimize the complexity and development cost of such solution.

Other aspects, features and advantages of the present invention are included in the following description of a representative embodiment, which description should be taken in conjunction with the accompanying drawing illustrating a schematic block diagram of network elements embodying the invention.

DESCRIPTION OF THE EMBODIEMENT :

As shown in the single Figure 1, its is proposed according to the invention to re-use the MIKEY protocol that is intended to secure key distribution over a network in order to secure keys exchange between the smartcard and a terminal over their local interface.

The traffic keys (in a encrypted form) needed to decrypt/descramble the content are generated by the broadcasting or diffusion center, or more generally a content delivery center, BM-SC and are sent to the terminal ME. These traffic keys are encrypted by using the so-called MIKEY Protocol defined for the real-time transmission/exchange of keys.

These encrypted traffic keys are sent jointly with the encrypted (or scrambled) content. These encrypted traffic keys are received by the terminal ME and sent to the secure token USIM. The secure token (for example a smartcard) decrypts the encrypted traffic keys received from the center through the terminal ME and sends the decrypted traffic keys, after encrypting them, to the terminal ME. As mentioned previously, these traffic keys are produced at a given timing rate. For example an encrypted traffic key is decrypted every 30 seconds by the card to be used by the terminal ME to decrypt/descramble the received content for a next time period of 30 seconds, and so on. So the encrypted traffic keys encrypted by the MIKEY protocol as received from the center through the terminal ME are decrypted by the secure token USIM and then re-encrypted - using the pre-shared scheme of the MIKEY Protocol - by the secure token to be sent to the terminal ME.

Thus according to the invention, the decrypted traffic keys produced by the token USIM are thus sent to the terminal ME in an encrypted form, after being re-encrypted using the MIKEY protocol. The terminal ME decrypts them to recover successive traffic keys in clear format to decrypt the content received from the center BM-SC.

MIKEY Protocol is defined by the Internet Engineering Task Force (IETF) in Document RFC 3830, such Document being hereby fully incorporated in the present application by this reference.

MIKEY Protocol defines three different methods of transporting/establishing a TGK key with the use of a pre-shared key, public-key encryption, and Diffie-Hellman (DH) key exchange.

Advantageously, the pre-shared key scheme of MIKEY is used for the transportation of traffic keys between the secure token and the terminal ME.

So, in order to protect the sensitive data (i.e. traffic keys) that are exchanged on the local interface between the authentication token and the ME (or an application on the ME), the authentication token will use existing secure key distribution functions such as the MIKEY protocol to protect the traffic key exchange between the ME and the authentication token. Instead of sending the traffic key in clear to the terminal over the local interface, the smartcard will send the traffic key in an encrypted manner to the terminal (e.g. by means of a MIKEY message).

The MIKEY message will be protected using a local key that is shared between the ME and the authentication token. Such key may be derived using Generic Bootstrapping Architecture (GBA) based methods.

The condition to protect the traffic key (e.g. sending the traffic keys using MIKEY instead of sending the key in clear) may be configured on the smartcard by means of local policy or may be securely sent over the network (e.g. the network may indicate to the smartcard in a delivery message to send the traffic keys to terminals in a protected manner only).

Thus it is possible to protect only sensitive keys that are exchanged between the smartcard and the terminal, whereas with existing solutions like the Secure Authentication Channel protects defined in ETSI TS 102 484 all the traffic between the smartcard and the terminal (or smartcard application and terminal application) will be protected. Securing the whole traffic will generate lower performances issues due to the limited resources available in a smartcard compared to another processing devices and potentially incompatibilities with real time requirements needed for such applications, and will be much more difficult to implement and test and will hamper interoperability.

It is also possible by implementing the present invention to use a protocol that is already required to be supported instead of requiring the support of a completely new specification.

Advantageously, the content delivery center instructs in a protected manner the secure token.

The operation of the secure token may be based upon a secured indication from the server or is based on local policy in the secure token.

The secure token and the terminal advantageously uses the MIKEY protocol together with a local key that is shared between a secure token and a terminal.

CLAIMS:

1 – A method for the protection of keys sent from a secure token (USIM) to a terminal (ME), said keys being traffic keys (MTK) used to decrypt a portion of content received from a content delivery center (BM-SC), said traffic keys being sent from said content delivery center (BM-SC) to the secure token (USIM) via a terminal (ME) using the MIKEY protocol defined by IETF RFC 3830, said method comprising the steps of (a) – decrypting in the secure token encrypted traffic keys received from content delivery center thereby producing traffic keys, and decryption by the terminal (ME) of the content received from the content delivery center (BM-SC) by using said traffic keys, characterized in that said method further comprises the step of (b) - encrypting in the secure token, using the MIKEY protocol defined by IETF RFC 4738, said traffic keys, and decryption by the terminal of said IETF RFC 3830-protocol-encrypted traffic keys.

2 – A method according to claim 1, wherein the encryption in the secure token of the traffic keys uses the pre-shared key scheme of the MIKEY protocol defined by IETF RFC 4738.

2 – Terminal for carrying out the method of claim 1.

3 – Secure token, for example smartcard, for carrying out the method of claim 1.

4 – Server for instructing in a protected manner the secure token for carrying out the method of claim 1.

5 – Secure token, for example smartcard, for carrying out the method of claim 1 based on a secured indication from the server.

6- Secure token, for example smartcard, for carrying out the method of claim 1 based on local policy in the secure token.

7- Secure token, for using the MIKEY protocol together with a local key that is shared between a secure token and a terminal.

8- Terminal, for using the MIKEY protocol together with a local key that is shared between a secure token and a terminal.

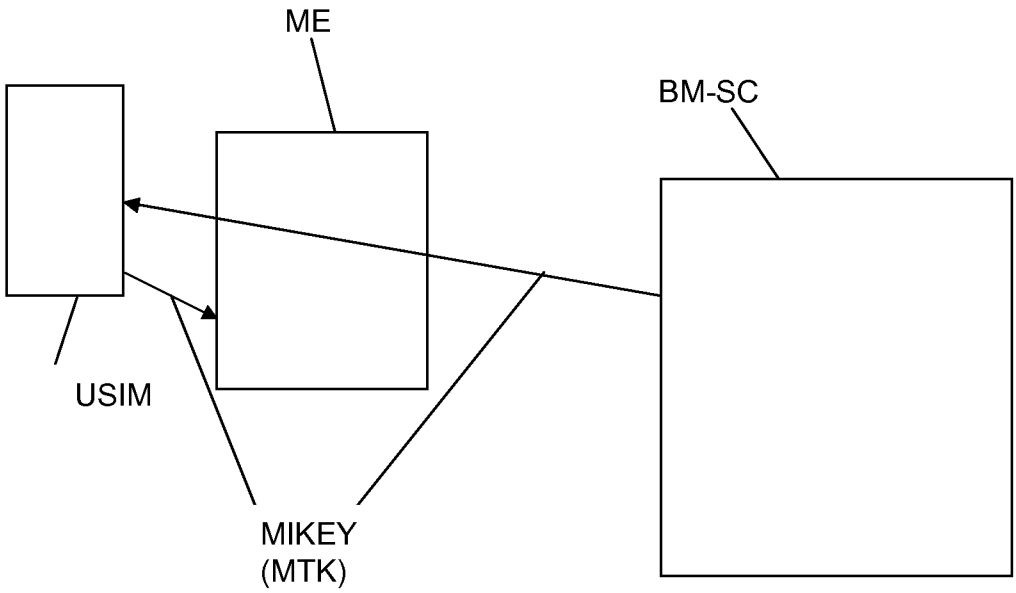

FIG.1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/054019

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 271 951 A (OCTALIS S A [BE]) 2 January 2003 (2003-01-02) the whole document	1-8
Y	US 2006/147040 A1 (LEE YUN K [KR] ET AL) 6 July 2006 (2006-07-06) the whole document	1-8
Y	US 2005/182971 A1 (ONG PENG T [SG] ET AL) 18 August 2005 (2005-08-18) the whole document	1-8
Y	WO 2004/019614 A (THOMSON LICENSING SA [FR]; SCHULTZ MARK ALAN [US]; CHIDAMBARAM DINAKAR) 4 March 2004 (2004-03-04) the whole document	1-8

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 May 2009	05/06/2009

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	Luckett, Paul

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/054019

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/048900 A1 (KIM CHAN-YONG [KR] ET AL) 13 March 2003 (2003-03-13) the whole document	1-8
Y	WO 97/38530 A (DIGCO B V [NL]; RIX SIMON PAUL ASHLEY [ZA]; GLASSPOOL ANDREW [GB]; DAV) 16 October 1997 (1997-10-16) the whole document	1-8

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/054019

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1271951 A	02-01-2003	WO 03001807 A1	03-01-2003
		US 2006179489 A1	10-08-2006
US 2006147040 A1	06-07-2006	JP 2006527865 T	07-12-2006
US 2005182971 A1	18-08-2005	WO 2005088524 A1	22-09-2005
WO 2004019614 A	04-03-2004	AU 2003258277 A1	11-03-2004
US 2003048900 A1	13-03-2003	CN 1407623 A	02-04-2003
		DE 10232348 A1	27-03-2003
		FR 2829266 A1	07-03-2003
		KR 20030018679 A	06-03-2003
WO 9738530 A	16-10-1997	AT 193963 T	15-06-2000
		AU 2506397 A	29-10-1997
		BR 9708500 A	03-08-1999
		CN 1215528 A	28-04-1999
		DE 69702310 D1	20-07-2000
		DE 69702310 T2	18-01-2001
		DK 891670 T3	30-10-2000
		ES 2149585 T3	01-11-2000
		HK 1019683 A1	17-09-2004
		HR 970160 A2	28-02-1998
		JP 2000508482 T	04-07-2000
		PT 891670 E	29-12-2000
		US 6385317 B1	07-05-2002
		ZA 9702786 A	23-10-1997