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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 November 2009 (12.11.2009)

PCT

(10) International Publication Number
WO 2009/136848 A1

(51) International Patent Classification:
G06F 21/24 (2006.01) *H04L 9/32* (2006.01)
G06Q 20/00 (2006.01)

(21) International Application Number:
PCT/SE2009/050466

(22) International Filing Date:
30 April 2009 (30.04.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0800997-9 5 May 2008 (05.05.2008) SE

(71) Applicant *(for all designated States except US)*: **PAYSYSTEM SWEDEN AB** [SE/SE]; P.O. Box 79, S-131 07 Nacka (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MOHSS, Anders** [SE/SE]; Västanåker 38, S-824 92 Hudiksvall (SE). **SAMILS, Henrik** [SE/SE]; Vretgränd 19, S-SE-753 22 Uppsala (SE).

(74) Agents: **BRANN AB** et al.; P.O. Box 17192, S-104 62 Stockholm (SE).

(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))*

[Continued on next page]

(54) **Title**: ELECTRONIC PAYMENTS IN A MOBILE COMMUNICATION SYSTEM

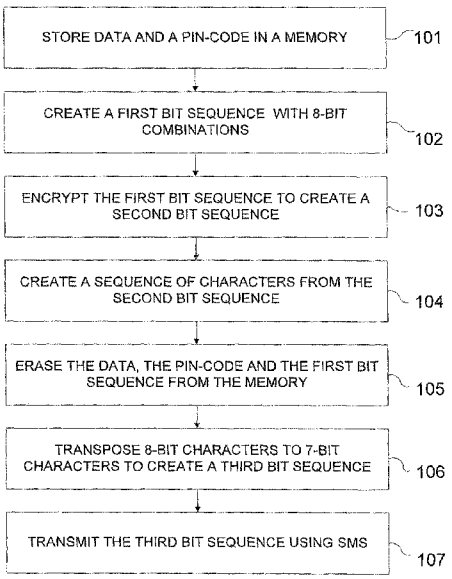

Fig. 1

(57) **Abstract**: The present invention relates to electronic payments in a mobile communication system. In particular, the present invention relates to methods and arrangements for secure transmission using SMS in a mobile communication system. In a method according to the invention data and a PIN-code are stored in a memory in a mobile terminal. A first bit sequence is created from the data and the PIN- code where different 8-bit combinations represent each character of the data and the PIN-code. Next the first bit sequence is encrypted using a PKI (Public Key Infrastructure)public-key to create a second bit sequence. A sequence of characters is then created from the second bit sequence, where each character in the sequence of characters is represented by an 8-bit combination. The characters are then transposed to 7-bit characters to create a third bit sequence which is transmitted to a server using SMS. The data, the PIN-code and the first bit sequence are also erased from the memory in the mobile terminal.

WO 2009/136848 A1

Published:

— *with international search report (Art. 21(3))*

Electronic payments in a mobile communication system

TECHNICAL FIELD

The present invention relates to methods and arrangements in a mobile telecommunication system. In particular it relates to methods and arrangements for secure transmission in the mobile telecommunication system.

BACKGROUND

The development of mobile terminals has over the past years been very rapid and today's mobile terminals support many different services e.g. MMS (Multimedia Messaging Service) and video calls besides ordinary phone calls. To be able to support these services today's mobile terminals often have several different radio access technologies e.g. GSM (Global System for Mobile communications), UMTS (Universal Mobile Telecommunications System) and WiFi. The mobile terminals also have several different ways of transporting data over these radio access technologies e.g. WAP (Wireless Application Protocol) and TCP/IP (Transmission Control Protocol/Internet Protocol). Even if today's mobiles terminals have support for advanced services, have many different radio access technologies and support different protocols for transporting data there are still many mobile terminals sold that do not support data transmission. If a service provider wants to provide a service that can be used from all mobile terminals the service provider also has to consider the mobile terminals already sold and what capabilities they have. A service provider is therefore confronted with a problem how the service should be provided so that it can be used from so many mobile terminals as possible.

Over the latest years the use of cash when performing payments has been reduced significantly. Instead, people use credit cards when paying in the shops and different electronic payment solutions when paying on the Internet. One of

the main problems with credit cards and other different electronic payment solutions is how to provide a secure solution. Matters that have been addressed before is for instance how to protect credit card numbers and other sensitive information when used on the Internet. As mentioned above today's mobile terminals also have data transmission capabilities which mean that they also can be used for Internet services, including different payments solutions. A further problem when using a mobile terminal in an electronic payment solutions is that the mobile terminal easily can be stolen or lost, which could lead to that sensitive information stored in the mobile terminal, like for instance credit card information, could be lost and used by a forger. Yet another problem when using a mobile terminal in an electronic payment solution is that information transmitted from the mobile terminal can be eavesdropped and used by a forger.

SUMMARY

It is therefore an object of the present invention to provide an improved solution for electronic payments in a mobile telecommunication system for obviating at least some of the above mentioned problems. The inventive solution to this end intends to use an SMS-message encrypted with a public key in order to be able to perform payments and to verify a sender of the SMS-message. By using a public key for the encryption a more secure solution is provided since no private key needs to be stored in the mobile terminal. Another advantage achieved by using a public encryption key is that all mobile terminals can use the same public encryption key. An exchange of encryption keys is therefore not necessary before a SMS-message is sent from the mobile terminal.

According to a first aspect of the embodiments of the present invention, the above stated problem is solved by means of a method for enabling a mobile terminal to securely transmit data and a PIN-code (Personal Identification Number) to a server. The method comprises: storing the data and the PIN-code in a memory in the mobile terminal; creating a first bit sequence where different 8-bit combinations represent each character of the data and the PIN-code;

encrypting the first bit sequence using a PKI (Public Key Infrastructure) public-key to create a second bit sequence; creating a sequence of characters from the second bit sequence by using a Base64 encoder, where each character in the sequence of characters is represented by an 8-bit combination. The method further comprises erasing the data, the PIN-code and the first bit sequence from the memory; transposing each 8-bit character in the sequence of characters to a 7-bit character to create a third bit sequence and transmitting the third bit sequence using SMS to the server.

According to a second aspect of the embodiments of the present invention, the above stated problem is solved by means of a mobile terminal for secure transmission of data and a PIN-code to a server wherein the mobile terminal comprises; a memory for storing the data and the PIN-code in the mobile terminal; creating means for creating a first bit sequence where different 8-bit combinations represent each character of the data and the PIN-code; encryption means for encrypting the first bit sequence using a PKI public-key to create a second bit sequence. The mobile terminal further comprises creating means for creating a sequence of characters from the second bit sequence by using a Base64 encoder, where each character in the sequence of characters is represented by an 8-bit combination; erasing means for erasing the data, the PIN-code and the first bit sequence from the memory; transposing means for transposing each 8-bit character in the sequence of characters to a 7-bit character to create a third bit sequence and a transmitter (36) for transmitting the third bit sequence using SMS (Short Message Service) to the server.

According to a third aspect of the embodiments of the present invention, the above stated problem is solved by means of a method for enabling a server to decrypt data and a first PIN-code and to verify a sender of said data and said PIN-code. The method comprises: receiving in an SMS message a third bit sequence comprising a sequence characters, where each character is represented by a 7-bit combination; transposing each 7-bit character in the sequence of

characters to an 8-bit character; creating a second bit sequence from the sequence of characters by using a Base64 decoder; retrieving a phone number from which the data and the PIN-code was sent and finding in the server a second PIN-code and a PKI private key associated with the phone-number; decrypting (205) the second bit sequence using the PKI private-key to create a first bit sequence. The method further comprises creating the data and the PIN-code from the first bit sequence, where each character in the PIN-code and the data is represented by an 8-bit combination and verifying the sender by comparing the first PIN-code and the second PIN-code.

According to a fourth aspect of the embodiments of the present invention, the above stated problem is solved by means of a server for decrypting data and a first PIN-code and for verifying a sender of the data and the PIN-code, wherein the server comprises: a receiver for receiving in an SMS message a third bit sequence comprising a sequence of characters, where each character is represented by a 7-bit combination; transposing means for transposing each 7-bit character in the sequence of characters to an 8-bit character; creating means for creating a second bit sequence from the sequence of characters by using a Base64 decoder; retrieving means for retrieving a phone number from which the data and the PIN-code was sent and finding in the server a second PIN-code and a PKI private key associated with the phone-number. The method further comprises decrypting means for decrypting the second bit sequence using the PKI private-key to create a first bit sequence; creating means for creating the data and the PIN-code from the first bit sequence, where each character in the PIN-code and the data is represented by an 8-bit combination and verifying means for verifying the sender by comparing the first PIN-code and the second PIN-code.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a method according to embodiments of the present invention.

Fig. 2 illustrates a method according to embodiments of the present invention.

Fig. 3 schematically illustrates a mobile terminal according to embodiments of the present invention.

Fig. 4 schematically illustrates a server according to embodiments of the present invention.

DETAILED DESCRIPTION

The foregoing and other objects, features and advantages of the invention will be apparent from the following detailed description of preferred embodiments.

The present invention sets forth methods and arrangements for performing payments in a mobile telecommunications system. The basic idea of the present invention is to utilize the fact that almost every mobile terminal supports SMS transmission which means that a payment solution provided via SMS can be used from almost every mobile terminal. The present invention also utilizes that sensitive information should be minimized in the mobile terminal and if the sensitive information is inserted in the mobile terminal the sensitive information should be erased from the mobile terminal after being used in the payment solution. Sensitive information should also be encrypted when transmitted from the mobile terminal. This would not only mean a payment solution that could be used from almost every mobile terminal but it will also facilitate a secure solution that prevents the sensitive information from being lost or eavesdropped and used by a forger.

Referring to figure 1, one aspect of the present invention relates to a method, which is illustrated by a flow chart in figure 1, for enabling a mobile terminal to securely transmit data and PIN-code to a server. The server can for instance be a server used in an electronic payment solution. The data and the PIN-code can be used for an economic transaction or an identification of a user. The economic transaction may for instance imply that money is being transferred from one bank account to another bank account or a payment for a specific item identified

by the data. Initially, a user of the mobile terminal enters the data and the PIN-code in the mobile terminal. In step 101, the data and the PIN-code are stored in a memory in the mobile terminal. If the data relates to, for instance an economic transaction, where money should be transferred from one subscriber to another subscriber the data may comprise a phone number to a receiver of the money, and a sum e.g. 100 indicating that the amount 100 should be transferred from an account associated with the user to an account associated with the receiver of the money. In the next step 102, a first bit sequence is created from the data and the PIN-code where each character in the data and the PIN-code is represented by different 8-bit combinations. If the data and the PIN-code for instance comprise 22 characters the first bit sequence will be 176 bits long. The data and the PIN-code have now been transformed to the first bit sequence in step 102. In step 103 the first bit sequence is encrypted using a PKI public-key to create a second bit sequence. Encryption in step 103 may be accomplished by using RSA up to 1024-bit encryption. According to one embodiment of the invention the second bit sequence is created with a maximum length of 1280 bits in step 103. Next in step 104, a sequence of characters is created from the second bit sequence by using a base 64 encoder, where each character is represented by an 8-bit combination. To ensure that no sensitive information is left in the memory after the method has been accomplished the data, the PIN-code and the first bit sequence are erased from the memory in step 105. To be able to send the sequence of characters by using SMS each character in the sequence of characters is transposed from 8-bit characters to 7-bit characters to create a third bit sequence. Finally the third bit sequence is transmitted to the server using SMS in step 107. The third bit sequence may be transmitted in several separate SMS-messages.

Another aspect of the present invention relates to a method, fig. 2, for enabling a server to decrypt data and a first PIN-code and to verify a sender of the data and the first PIN-code. The server can for instance be a server in an electronic payment solution. The electronic payment solution may comprise an economic transaction which may imply that money is being transferred from one bank

account to another bank account or a payment for a specific item specified by the data. In the first step 201, a third bit sequence comprising a sequence of characters is received in an SMS message. Each character in the sequence is represented by a 7-bit combination. Next, in the step 202, each 7-bit character in said sequence of characters is transposed to an 8-bit character. In the step 203 a second bit sequence is created from the sequence of characters by using a Base64 decoder. In step 204, a phone number from which said data and said first PIN-code were sent is retrieved from said server. Step 204 further comprises finding, in said server, a second PIN-code and a PKI private key associated with said phone-number. The PKI private key is used in step 205 to decrypt the second bit sequence to create a first bit sequence. From the first bit sequence, the data and the first PIN-code are created in step 206, where each character in the data and the first PIN-code is represented by an 8-bit combination. Finally the sender is verified in step 207 by comparing the first PIN-code and the second PIN-code.

Yet another aspect of the present invention relates to a mobile terminal 37 for secure transmission of data and a PIN-code to a server. The mobile terminal 37, is illustrated in figure 3. The server may be a server in an electronic payment solution. A memory is 30 is provided in the mobile terminal 37 for storing the data and the PIN-code in the mobile terminal. Creating means 31 is also provided in the mobile terminal 37 for creating a first bit sequence where different 8-bit combinations represent each character of the data and the PIN-code. In addition the mobile terminal 37 further comprises encryption means 32 for encrypting the first bit sequence using a PKI public-key to create a second bit sequence. The encryption means may be further configured for creating the second bit sequence with a maximum length of 1280 bits. According to other embodiments of the invention the encryption means may also be further configured for encrypting using RSA up to 1024-bit encryption. The mobile terminal 37 further comprises creating means 33 for creating a sequence of characters from the second bit sequence by using a Base64 encoder, where each character in the sequence of characters is represented by an 8-bit combination.

The mobile terminal 37 also comprises erasing means 34 for erasing the data, the PIN-code and the first bit sequence from the memory means 30 and transposing means for transposing each 8-bit character in the sequence of characters to a 7-bit character to create a third bit sequence. Finally, transmitting means 36 in the mobile terminal 37 is provided for transmitting the third bit sequence using SMS to the server. The third bit sequence may be transmitted in several separate SMS-messages by the transmitting means 36.

Referring to figure 4, another aspect of the present invention relates to a server for decrypting data and a first PIN-code and for verifying a sender of the data and the first PIN-code. The server may be a server in an electronic payment solution. The server 47 comprises receiver means 40 for receiving in an SMS message a third bit sequence comprising a sequence of characters, where each character is represented by a 7-bit combination. The server 47 comprises further transposing means 41 for transposing each 7-bit character in said sequence of characters to an 8-bit character and creating means 42 in the server is provided for creating a second bit sequence from said sequence of characters by using a Base64 decoder. In addition, retrieving means 43 is provided in the server 47 for retrieving from a memory 48 a phone number from which the data and the PIN-code was sent. The retrieving means 43 is also configured to find in said memory 48 a second PIN-code and a PKI private key associated with the phone-number in the server. The server 47 also comprises decrypting means 44 for decrypting the second bit sequence using the PKI private-key to create a first bit sequence. In order to create the data and the first PIN-code from the first bit sequence the creating means 45 is also provided in the server 47, where each character in the PIN-code and the data is represented by an 8-bit combination. Finally, the server comprises verifying means 46 in the server for verifying the sender by comparing the first PIN-code and the second PIN-code.

The means mentioned in the present description can be software means, hardware means or a combination of both. The described subject matter is of

course not limited to the above described and in the drawings shown embodiments, but can be modified within the scope of the enclosed claims.

CLAIMS

1. A method for enabling a mobile terminal to securely transmit data and a Personal Identification Number-code, PIN-code, to a server, the method comprises;

-storing (101) the data and the PIN-code in a memory in the mobile terminal;

-creating (102) a first bit sequence where different 8-bit combinations represent each character of said data and said PIN-code;

-encrypting (103) said first bit sequence using a Public Key Infrastructure public-key, PKI public-key, to create a second bit sequence;

-creating (104) a sequence of characters from said second bit sequence by using a Base64 encoder, where each character in the sequence of characters is represented by an 8-bit combination.

-erasing (105) the data, the PIN-code and the first bit sequence from the memory;

-transposing (106) each 8-bit character in said sequence of characters to a 7-bit character to create a third bit sequence; and

-transmitting (107) said third bit sequence using Short Message Service, SMS, to the server.

2. A method according to claim 1, wherein said step of encrypting further comprises creating said second bit sequence with a maximum length of 1280 bits.

3. A method according to any of previous claims, wherein said step of encrypting is accomplished by using RSA up to 1024-bit encryption.

4. A method according to any of previous claims, wherein said step of transmitting using SMS, further comprises transmitting said third bit sequence in several separate SMS-messages.

5. A method according to any of previous claims, wherein said data is used for an economic transaction or an identification of a user.

6. A method according to any of previous claims, wherein said server is a server in an electronic payment solution.

7. A method for enabling a server to decrypt data and a first Personal Identification Number-code, PIN-code, and to verify a sender of said data and said first PIN-code the method comprises;

- receiving (201) in an Short Message Service message, SMS-message, a third bit sequence comprising a sequence characters, where each character is represented by a 7-bit combination;

- transposing (202) each 7-bit character in said sequence of characters to an 8-bit character;

- creating (203) a second bit sequence from said sequence of characters by using a Base64 decoder;

- retrieving (204) a phone number from which said data and said PIN-code was sent and finding in said server a second PIN-code and a Public Key Infrastructure private key, PKI private key, associated with said phone-number;

- decrypting (205) said second bit sequence using said PKI private-key to create a first bit sequence;

- creating (206) said data and said PIN-code from said first bit sequence, where each character in said PIN-code and said data is represented by an 8-bit combination; and

- verifying (207) the sender by comparing the first PIN-code and the second PIN-code.

8. A method according to claim 7, wherein said server is a server in an electronic payment solution.

9. A method according to any to claims 7 and 8, wherein said data is used for an economic transaction.

10. A mobile terminal (37) for secure transmission of data and a Personal Identification Number-code, PIN-code, to a server wherein said mobile terminal comprises;

a memory (30) for storing the data and the PIN-code in the mobile terminal;

creating means (31) for creating a first bit sequence where different 8-bit combinations represent each character of said data and said PIN-code;

encryption means (32) for encrypting said first bit sequence using a Public Key Infrastructure public-key, PKI public-key, to create a second bit sequence;

creating means (33) for creating a sequence of characters from said second bit sequence by using a Base64 encoder, where each character in the sequence of characters is represented by an 8-bit combination.

erasing means (34) for erasing the data, the PIN-code and the first bit sequence from the memory;

transposing means (35) for transposing each 8-bit character in said sequence of characters to a 7-bit character to create a third bit sequence; and

a transmitter (36) for transmitting said third bit sequence using Short Message Service, SMS, to the server.

11. A mobile terminal (37) according to claim 10, wherein said encryption means is further configured for creating said second bit sequence with a maximum length of 1280 bits.

12. A mobile terminal according to claims 10 or 11, wherein said encryption means is further configured for encrypting using RSA up to 1024-bit encryption.

13. A mobile terminal according to any of claims 9 to 12, wherein said server is a server in an electronic payment solution.

14. A server (47) for decrypting data and a first Personal Identification Number code, PIN-code, and for verifying a sender of said data and said first PIN-code, wherein said server comprises;

a receiver (40) for receiving in an Short Message Service message, SMS-message, a third bit sequence comprising a sequence of characters, where each character is represented by a 7-bit combination;

transposing means (41) for transposing each 7-bit character in said sequence of characters to an 8-bit character;

creating means (42) for creating a second bit sequence from said sequence of characters by using a Base64 decoder;

retrieving means (43) for retrieving a phone number from which said data and said first PIN-code was sent and finding a second PIN-code and a Public Key Infrastructure private key, PKI private key, associated with said phone-number;

decrypting means (44) for decrypting said second bit sequence using said PKI private-key to create a first bit sequence;

creating means (45) for creating said data and said first PIN-code from said first bit sequence, where each character in said PIN-code and said data is represented by an 8-bit combination; and

verifying means (46) for verifying the sender by comparing the first PIN-code and the second PIN-code.

15. A server according to claim 14, wherein said server is a server in an electronic payment solution.

16. A server according to claim 14 or 15, wherein said data is used for an economic transaction.

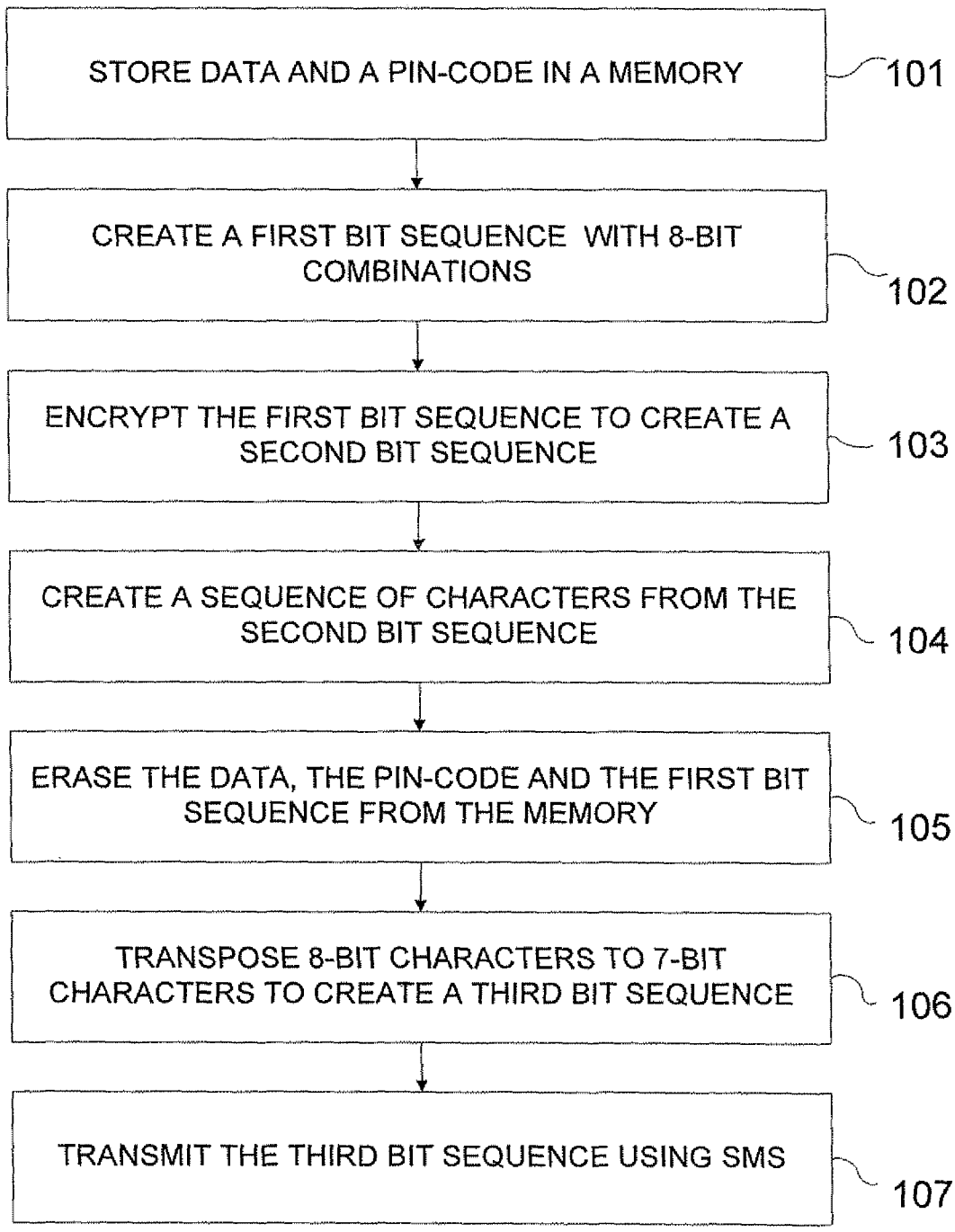
STORE DATA AND A PIN-CODE IN A MEMORY
101
CREATE A FIRST BIT SEQUENCE WITH 8-BIT COMBINATIONS
102
ENCRYPT THE FIRST BIT SEQUENCE TO CREATE A SECOND BIT SEQUENCE
103
CREATE A SEQUENCE OF CHARACTERS FROM THE SECOND BIT SEQUENCE
104
ERASE THE DATA, THE PIN-CODE AND THE FIRST BIT SEQUENCE FROM THE MEMORY
105
TRANSPOSE 8-BIT CHARACTERS TO 7-BIT CHARACTERS TO CREATE A THIRD BIT SEQUENCE
106
TRANSMIT THE THIRD BIT SEQUENCE USING SMS
107

Fig. 1

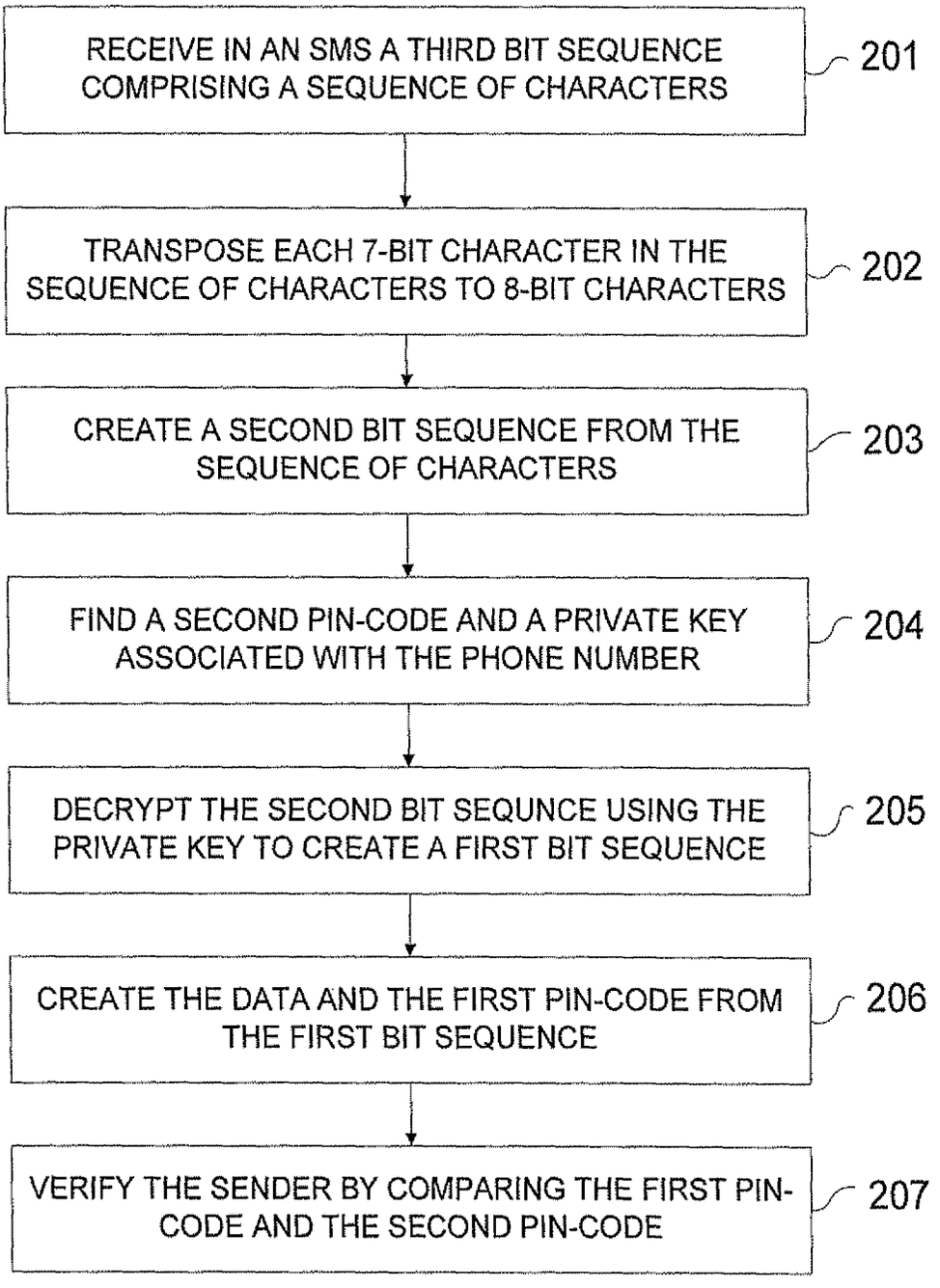
RECEIVE IN AN SMS A THIRD BIT SEQUENCE COMPRISING A SEQUENCE OF CHARACTERS
201
TRANSPOSE EACH 7-BIT CHARACTER IN THE SEQUENCE OF CHARACTERS TO 8-BIT CHARACTERS
202
CREATE A SECOND BIT SEQUENCE FROM THE SEQUENCE OF CHARACTERS
203
FIND A SECOND PIN-CODE AND A PRIVATE KEY ASSOCIATED WITH THE PHONE NUMBER
204
DECRYPT THE SECOND BIT SEQUNCE USING THE PRIVATE KEY TO CREATE A FIRST BIT SEQUENCE
205
CREATE THE DATA AND THE FIRST PIN-CODE FROM THE FIRST BIT SEQUENCE
206
VERIFY THE SENDER BY COMPARING THE FIRST PIN-CODE AND THE SECOND PIN-CODE
207

Fig. 2

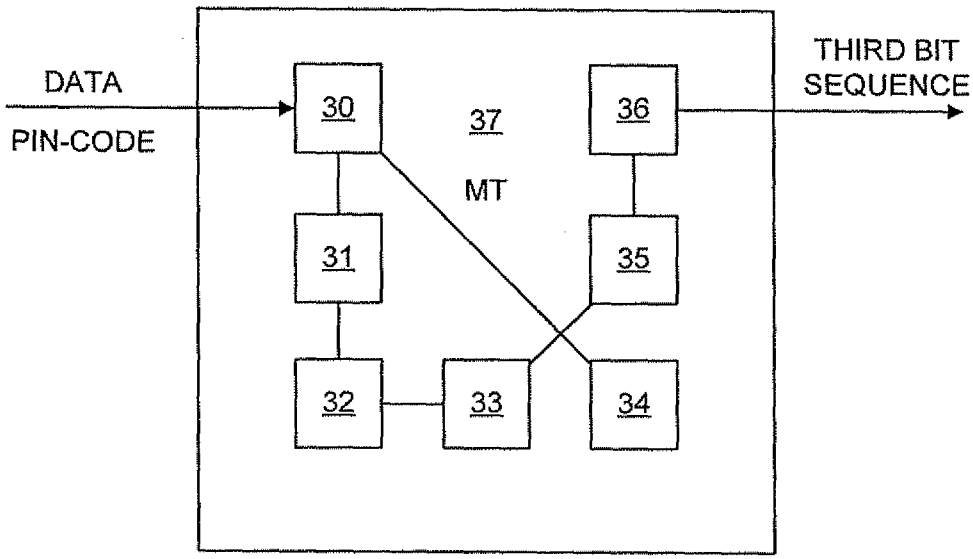
DATA
PIN-CODE
30
37
MT
36
THIRD BIT
SEQUENCE
31
35
32
33
34

Fig. 3

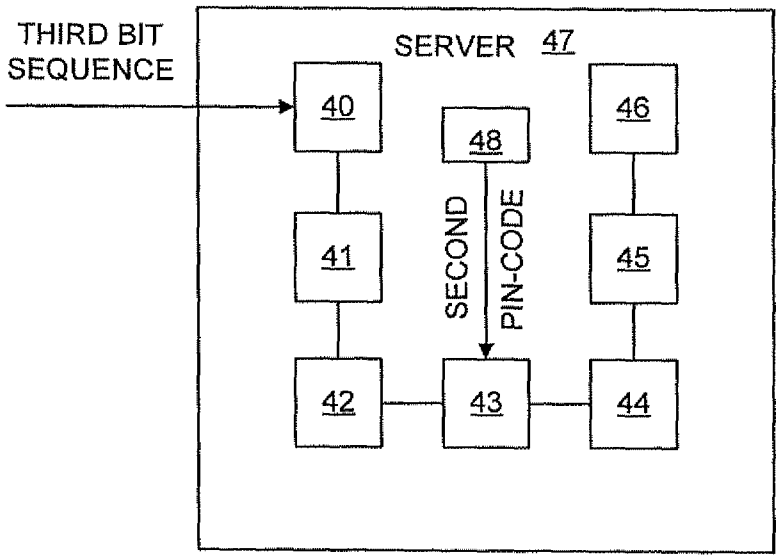
THIRD BIT
SEQUENCE
SERVER 47
40
48
46
SECOND
PIN-CODE
41
45
42
43
44

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/050466

A. CLASSIFICATION OF SUBJECT MATTER

IPC: 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: G06F, G06Q, H04L

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

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ, COMPDX, INSPEC, XPI3E

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2372867 A (SONERA SMARTTRUST LTD), 4 Sept 2002 (04.09.2002), page 14, line 8 - page 16, line 20; page 21, line 16 - page 26, line 2, abstract --	1-16
A	WO 03015343 A1 (NEXSE S.R.L.), 20 February 2003 (20.02.2003), page 2, line 32 - page 4, line 13; page 8, line 18 - page 10, line 20, abstract --	1-16
A	US 20060019634 A1 (HAWKES M.), 26 January 2006 (26.01.2006), abstract, paragraphs [0004],[0006], [0015],[0038],[0042],[0046]-[0051] --	1-16

[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
12 June 2009	16 -06- 2009
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Frida Holmberg/ELY Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/050466

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 03096615 A1 (WIRELESS APPLICATIONS PTY LTD), 20 November 2003 (20.11.2003), page 2, line 1 - page 3, line 28, figures 3,4, abstract -- --------	1-16

International patent classification (IPC)

G06F 21/24 (2006.01)
G06Q 20/00 (2006.01)
H04L 9/32 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded:

- From "Cited documents" found under our online services at www.prv.se (English version)
- From "Anförda dokument" found under "e-tjänster" at www.prv.se (Swedish version)

Use the application number as username. The password is **TAHHSEVRBH.**

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

GB	2372867	A	04/09/2002	NONE			
WO	03015343	A1	20/02/2003	IT	RM20010492	A	10/02/2003
US	20060019634	A1	26/01/2006	NONE			
WO	03096615	A1	20/11/2003	CN	1653746	A	10/08/2005
				EP	1502383	A	02/02/2005
				US	20060098678	A	11/05/2006