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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 March 2008 (20.03.2008)

PCT

(10) International Publication Number
WO 2008/033065 A1

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

(21) International Application Number:
PCT/SE2007/000672

(22) International Filing Date: 9 July 2007 (09.07.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0601905-3 15 September 2006 (15.09.2006) SE

(71) Applicant *(for all designated States except US)*: **COMFACT AB** [SE/SE]; Box 2324, S-403 15 Göteborg (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **TÖRNQVIST, Anders** [SE/SE]; Norra Liden 23, S-411 18 Göteborg (SE).

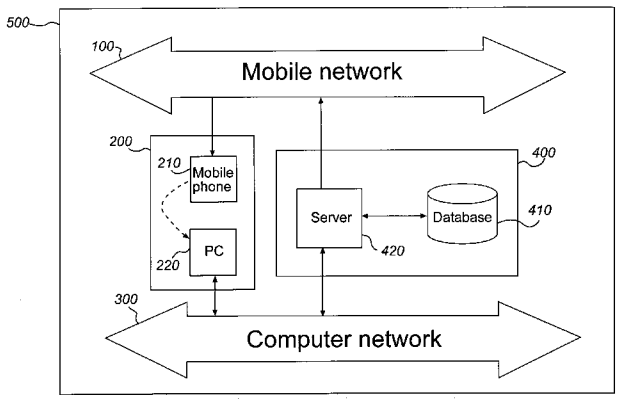
(74) Agent: **AWAPATENT AB**; Box 11394, S-404 28 Göteborg (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, 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, 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, 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, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(54) **Title:** METHOD AND COMPUTER SYSTEM FOR ENSURING AUTHENTICITY OF AN ELECTRONIC TRANSACTION



(57) **Abstract:** The present invention relates to a method for ensuring authenticity of an electronic transaction performed during a transaction session, comprising the steps of receiving, over a first network, a request from a user for the completion of an electronic transaction, receiving, over the first network, an authentication code from the user which has been provided to the user over a second network separated from the first network, thereby authenticating the user, completing the electronic transaction, and storing information associated with the electronic transaction and the transaction session. The method further comprises the step of generating a one-way hash value based on information comprised in the electronic transaction and information associated with the transaction session, and providing the one-way hash value to the user, wherein the one-way hash value is usable for ensuring the authenticity of the electronic transaction. The procedure enables authentication, integrity, non-repudiation, and time stamping in a cost efficient way. An enhanced security level can be achieved as the network used for providing the authentication code to the user is separate from the network where the user returns the authentication code. The present invention also relates to a corresponding computer system adapted for ensuring the authenticity of an electronic transaction.

WO 2008/033065 A1

METHOD AND COMPUTER SYSTEM FOR ENSURING AUTHENTICITY OF AN ELECTRONIC TRANSACTION

Field of the invention

The present invention relates to a method for ensuring authenticity of an electronic transaction performed during a transaction session. The present invention also relates to a corresponding computer system adapted to ensure authenticity of an electronic transaction performed during a transaction session.

Description of the related art

Conventionally, a signature on a paper document is a way to connect a natural or legal person to a legal action such as for example an application, a report, a registration, or a sales contract. With the success of the Internet, many organizations such as municipalities, companies and banks tries to rationalize the handling of paper documents that requires a signature. In most cases this has been solved by providing documents on a web site from which it can be downloaded to be filled out and printed. The printed paper document is then signed and sent by regular mail to the receiver.

An electronic alternative that may further reduce the handling of paper documents is Public Key Infrastructure (PKI). This arrangement binds public keys with respective user identities by means of a certificate issued by a trusted third party, also known as a certificate authority (CA). Accordingly, electronic transactions can be signed in a way which provides:

- authentication (i.e. make it possible to identify the source of a message), and
- integrity (i.e. ensures that the transaction has not been changed after it was signed).

PKI may also provide non-repudiation (i.e. prevent the act of disclaiming responsibility for a message) unless the user repudiates his signature key. To provide certainty about the date and time at which the underlying document was signed, the PKI-solution may be combined with trusted time stamping. However, a disadvantage when using a large scale PKI-solution is that it can be highly complicated and expensive for an organization.

A possible simpler solution is suggested in WO 99/44114, disclosing an arrangement for authenticating a user to an application, the application being available to the user through a first communications network, and the user is provided the possibility to be authenticated to the application by means of a mobile station communicating through a second communications network.

Another solution is suggested in WO 99/05628, disclosing an electronic bill presentment and payment system. Here, a biller computer stores complete bills for the customer. A bill presentment computer stores a summary of each complete bill along with a hash of that complete bill which is digitally signed by the biller computer. A customer computer makes a payment on a complete bill by generating a payment message which includes the hash of the selected complete bill digitally signed by the biller computer which is digitally signed by that particular customer computer. The payment message is stored in a closing record for use in resolving issues regarding whether or not the bill was changed after payment was authorized, and whether or not an alleged payment on the selected bill was authorized.

However, none of the prior art documents provides a cost efficient solution for ensuring authenticity, integrity, non-repudiation, and time stamping.

Object of the invention

There is therefore a need for an improved method for ensuring authenticity, integrity, non-repudiation, and time stamping of an electronic transaction, and more specifically that handles the costly implementations in accordance with prior art.

Summary of the invention

According to an aspect of the invention, the above object is met by a method for ensuring authenticity of an electronic transaction performed during a transaction session, comprising the steps of receiving, over a first network, a request from a user for the completion of an electronic transaction, receiving, over the first network, an authentication code from the user which has been provided to the user over a second network separated from the first network, thereby authenticating the user, completing the electronic transaction, and storing information associated with the electronic transaction and the transaction session, wherein the method further comprises the step of

generating a one-way hash value based on information comprised in the electronic transaction and information associated with the transaction session, and providing the one-way hash value to the user, wherein the one-way hash value is usable for ensuring the authenticity of the electronic transaction.

The procedure enables authenticity of an electronic transaction, i.e. authentication, integrity, non-repudiation, and time stamping in a cost efficient way. Further, no prior contact between the parties is required, nor does the user need to have access to any equipment specially designed for the purpose. Other advantages associated with the procedure is that non-repudiation applies to both parties, and that both parties are provided with a verifiable proof of the authenticity of the electronic transaction. Furthermore, an enhanced security level can be achieved as the second network used for providing the authentication code to the user is separate from the first network where the user returns the authentication code. This involves active participation of the user in entering the received authentication code.

The present invention is based on the understanding that by generating a one-way hash value based on information comprised in the electronic transaction and on information associated with the transaction session, integrity, non-repudiation (for both parties), and time stamping (i.e. certainty about the date and time of the transaction) can be achieved.

Furthermore, authenticity of the user can be ensured by communicating with the user over two separate communication networks, as long as at least one of these can be tied to the identity of the user. Through the arrangement no prior contacts between the parties is required and standard equipment, such as a mobile phone and a computer having a network connection, is all that the user needs to have access to. The result is a cost efficient implementation compared to prior art arrangements.

Preferably, the first network can be a computer network and the second network can be a mobile network. This may be a convenient way to utilize standard equipment as the typical user has access to a personal computer connected to the Internet, and a mobile phone. A further advantage, in an embodiment where the authentication code is provided to the user's mobile phone, is that a verification of the user can be performed, for example, through information associated with the subscription of the mobile phone.

The authentication code, which may be a certificate and an associated one-way hash value, can advantageously be provided to the user by means

of an SMS or an MMS, but can also be provided by alternative means such as, for example, a voice message or a phone call to the user. As the mobile phone and its SIM-card, or similar, typically is protected with a PIN-code only known by the user, the mobile phone can here be used as a tool for providing user authentication, thereby reducing the risk of fraud.

In an embodiment, the one-way hash value may be included with a receipt for the electronic transaction. The one-way hash value typically serves as a verifiable proof of the authenticity of the electronic transaction, and the receipt may function as a meaningful label to the user. The receipt can include the complete content of the electronic transaction, and be displayed on the user terminal, or alternatively, for example, be received by email, SMS or MMS. If the hash value is based only on information that appears on the receipt, the authenticity of the receipt can be verified without requiring any additional information as long as the hash function is known.

Furthermore, the transaction session can be signed using a digital session certificate, which connects signature verification data (such as codes or public keys) used in the transaction session with the user. Thus, the identity of the user can be confirmed and the security level of the performed transaction is further enhanced.

In a preferred embodiment, the authentication code may be a one-way hash value generated based on information associated with the initial steps of the electronic transaction. Thus, the authentication code can be tied to the electronic transaction, thereby further increasing the security level of the electronic transaction.

According to a further aspect of the invention, there is provided a computer system adapted to ensure authenticity of an electronic transaction performed during a transaction session, the computer system comprising means for receiving, over a first network, a request from a user for the completion of an electronic transaction, means for receiving, over the first network, an authentication code from the user which has been provided to the user over a second network separated from the first network, thereby authenticating the user, means for completing the electronic transaction, and means for storing information associated with the electronic transaction and the transaction session, wherein the computer system further comprises means for generating a one-way hash value based on information comprised in the electronic transaction and information associated with the transaction session, and means for providing the one-way hash value to the user,

wherein the one-way hash value is usable for ensuring the authenticity of the electronic transaction. This aspect of the invention provides similar advantages as according to the above discussed.

Furthermore, the authentication code can be provided to the user by a third party communicatively connected to the computer system. This allows services to be divided between various service providers. For instance, the authentication code may be provided to the user by a mobile network operator. However, the computer system can also further comprise means for providing the authentication code over the second network.

Brief description of the drawings

These and other aspects of the present invention will now be described in more detail, with reference to the appended drawings showing currently preferred embodiments of the invention, in which:

Figure 1 is a block diagram illustrating a computer system according to an embodiment of the present invention; and

Figure 2 is a flow chart illustrating the fundamental steps of a method according to an embodiment of the present invention for ensuring authenticity of an electronic transaction.

Detailed description of currently preferred embodiments

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which currently preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiment are provided for thoroughness and completeness, and fully convey the scope of the invention to the skilled addressee. Like reference characters refer to like elements throughout.

Referring now to the drawings and to figure 1 in particular, there is depicted the main components in an embodiment of the invention. In figure 1, a network environment 500 provides a platform for a user and a service provider to interact and exchange information. The user has access to an arrangement 200 comprising a user terminal 220, for example in the form of a personal computer (PC) or a work station or a portable computer, and a portable electronic device 210, such as a mobile phone comprising a SIM-card or similar. The user terminal 220 is connected to a first network 300,

which is typically a computer network including for example a local area network (LAN) or a wide area network (WAN) such as the Internet, and the portable electronic device 210 is connected to a second network 100, for example in the form of a mobile network such as a GSM, a CDMA or similar mobile phone network.

The service provider administrates a computer system 400 adapted to ensure authenticity of an electronic transaction during a transaction session. The computer system 400 comprises a server 420 and a database 410. It is also provided with the possibility to connect to the computer network 300 and to the mobile network 100. Communication over the computer network 300, between the service provider and the user, can be secured as required by using a cryptographic protocol such as, for example, TLS (Transport Layer Security) or SSL (Secure Sockets Layer). Accordingly, the information can be encrypted and both parties can be authenticated. Furthermore, the server 420 may comprise, for example, a database management system utilizing SQL to access the database 410. The database 410 typically holds database records with information such as, for example, customer records and transaction records. These are preferably stored in a format such as XML.

Turning now to figure 2, which is a flow chart illustrating the fundamental steps of a method according to an embodiment of the present invention, a typical procedure according to the present invention is described. In a typical application of the invention, the user may access a web site through the web browser of the user terminal 220. The web site may provide a variety of services that involves electronic transactions such as, for example, purchasing goods or electronically signing a document. As the user is about perform a electronic transaction, a transaction session is initiated, as illustrated by step 901.

In order to complete the electronic transaction, the user submits, in step 902, a request for completion of the electronic transaction. As part of this request the user is prompted to enter user identification to identify himself. Depending on the application, this may include for example name, social security number, address, credit card number, mobile phone number, and customer number with the operator of the mobile network, or similar. The request for completion of the electronic transaction is then transmitted, over the computer network 300, from the user terminal 220 to the computer system 400 of the service provider.

After receiving the request for completion of the electronic transaction, the computer system 400 of the service provider initiates, in step 903, a verification process to verify the identity of the user. This is done by comparing the user identification in the received request for completion of the electronic transaction, to the information about the user stored in the database records in the database 410. As part of the verification process, the computer system 400 may also access and utilize external information. An example of this would be information registered in a subscription record of the user's mobile phone provided from a mobile network operator. Moreover, other information related to the transaction session may be used in the verification process, such as signature verification data associated with a digital session certificates for the transaction session.

If the user identification submitted by the user cannot be confirmed by the information in the database 410, or external information, the user is not allowed to complete the electronic transaction. Thus, in step 904, the transaction session is terminated and the user is informed thereof. The information can be conveyed to the user by displaying a message on the user terminal 220, or, alternatively, an SMS or MMS could be sent to the user's mobile phone 210.

If the user identification submitted by the user is confirmed, the user is considered to be authorized to complete the electronic transaction. Thus, in step 905, an authentication code is generated and sent to the user's mobile phone 210 over the mobile network 100, for instance, as an SMS or MMS. In addition to this, the authentication code is registered in the database records in the database 410. The authentication code may advantageously be a temporary and time limited digital session certificate. Typically, such a certificate is only valid for the ongoing transaction session and for the ongoing electronic transaction and for a limited time period, such as for example a 5 minute time period. In the case where the service provider is a Certificate Authority (CA), it can issue qualified certificates.

After receiving the authentication code, the user enters, in step 906, the authentication code in the web browser of the user terminal 220. The authentication code is then transmitted to the service provider over the computer network 300.

As the computer system 400 of the service provider receives the authentication code, in step 907, it is compared to the authentication code that was registered in the database records in the above described step 905.

If the received authentication code does not match the one stored in the database records, the user is not authorized to complete the electronic transaction. Hence, in step 908, the transaction session is terminated and the user is notified thereof over the computer network 300.

If the authentication code match the one registered in the database records, the electronic transaction is completed in step 909 and the database 410 is updated accordingly. This involves updating the database records with information about the electronic transaction such as, for example, first name, last name, amounts, codes, etc. In addition, the database records may also be updated with information associated with the transaction session, such as signature verification data, the hash value in the certificate, date, time, session identification and IP-address. Moreover, a string of characters representing the complete transaction is stored in the database records. This string of characters contains all relevant data of the electronic transaction as well as of the transaction session. This may include the total contents of the transaction, signature verification data, the hash value in the certificate, date, time, session identification and IP-address. If required, certain data can be omitted.

In step 910, a one-way hash value usable for ensuring the authenticity of the electronic transaction is generated from the string of characters of the transaction. This connects the user to the content of the transaction and the performed action. Examples of typical hash functions that may be used are MD5 or SHA-1.

In step 911, the complete content of the electronic transaction along with the one-way hash value thereof is sent to the user over the computer network 300, and displayed on the user terminal 220. The user may choose to print this as a receipt of the completed transaction, and a verification that it has been received by the service provider. The user can also chose to receive this information by email, to save it on the computer as a file, or to have the unique hash value sent to the user's mobile phone 210.

Finally, in step 912, the transaction session is completed.

The skilled addressee realizes that the present invention by no means is limited to the preferred embodiments described above. On the contrary, many modifications and variations are possible within the scope of the appended claims.

CLAIMS

1. A method for ensuring authenticity of an electronic transaction performed during a transaction session, comprising the steps of:

- receiving, over a first network, a request from a user for the completion of an electronic transaction;

- receiving, over the first network, an authentication code from the user which has been provided to the user over a second network separated from the first network, thereby authenticating the user;

- completing the electronic transaction; and

- storing information associated with the electronic transaction and the transaction session,

characterized in that the method further comprises the step of:

- generating a one-way hash value based on information comprised in the electronic transaction and information associated with the transaction session; and

- providing the one-way hash value to the user, wherein the one-way hash value is usable for ensuring the authenticity of the electronic transaction.

2. Method according to claim 1, wherein the first network is a computer network and the second network is a mobile network.

3. Method according to any of claims 1 or 2, wherein the one-way hash value is included with a receipt for the electronic transaction.

4. Method according to any one of the preceding claims, wherein the transaction session is signed using a digital session certificate.

5. Method according to any one of the preceding claims, wherein the authentication code is a one-way hash value generated based on information associated with the initial steps of the electronic transaction.

6. A computer system adapted to ensure authenticity of an electronic transaction performed during a transaction session, the computer system comprising:

- means for receiving, over a first network, a request from a user for the completion of an electronic transaction;

- means for receiving, over the first network, an authentication code from the user which has been provided to the user over a second network separated from the first network, thereby authenticating the user;

- means for completing the electronic transaction; and

- means for storing information associated with the electronic transaction and the transaction session,

characterized in that the computer system further comprises:

- means for generating a one-way hash value based on information comprised in the electronic transaction and information associated with the transaction session; and

- means for providing the one-way hash value to the user, wherein the one-way hash value is usable for ensuring the authenticity of the electronic transaction.

7. Computer system according to claim 6, wherein the first network is a computer network and the second network is a mobile network.

8. Computer system according to any of claims 6 or 7, wherein the one-way hash value is included with a receipt for the electronic transaction.

9. Computer system according to any of claims 6 – 8, wherein the computer system further comprises means for generating a digital session certificate for digitally signing the transaction session.

10. Computer system according to any of claims 6 – 9, wherein the authentication code is provided to the user by a third party communicatively connected to the computer system.

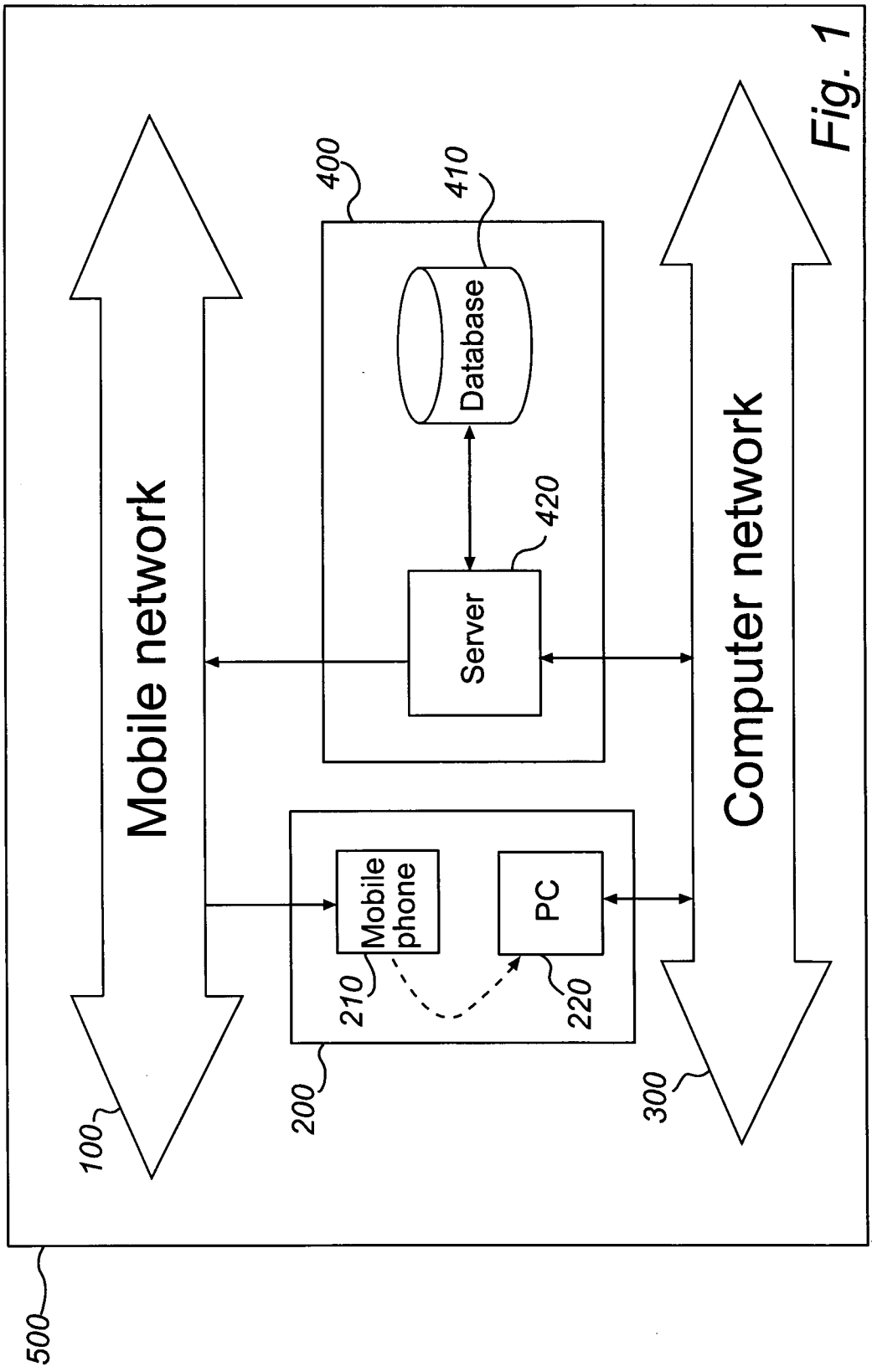
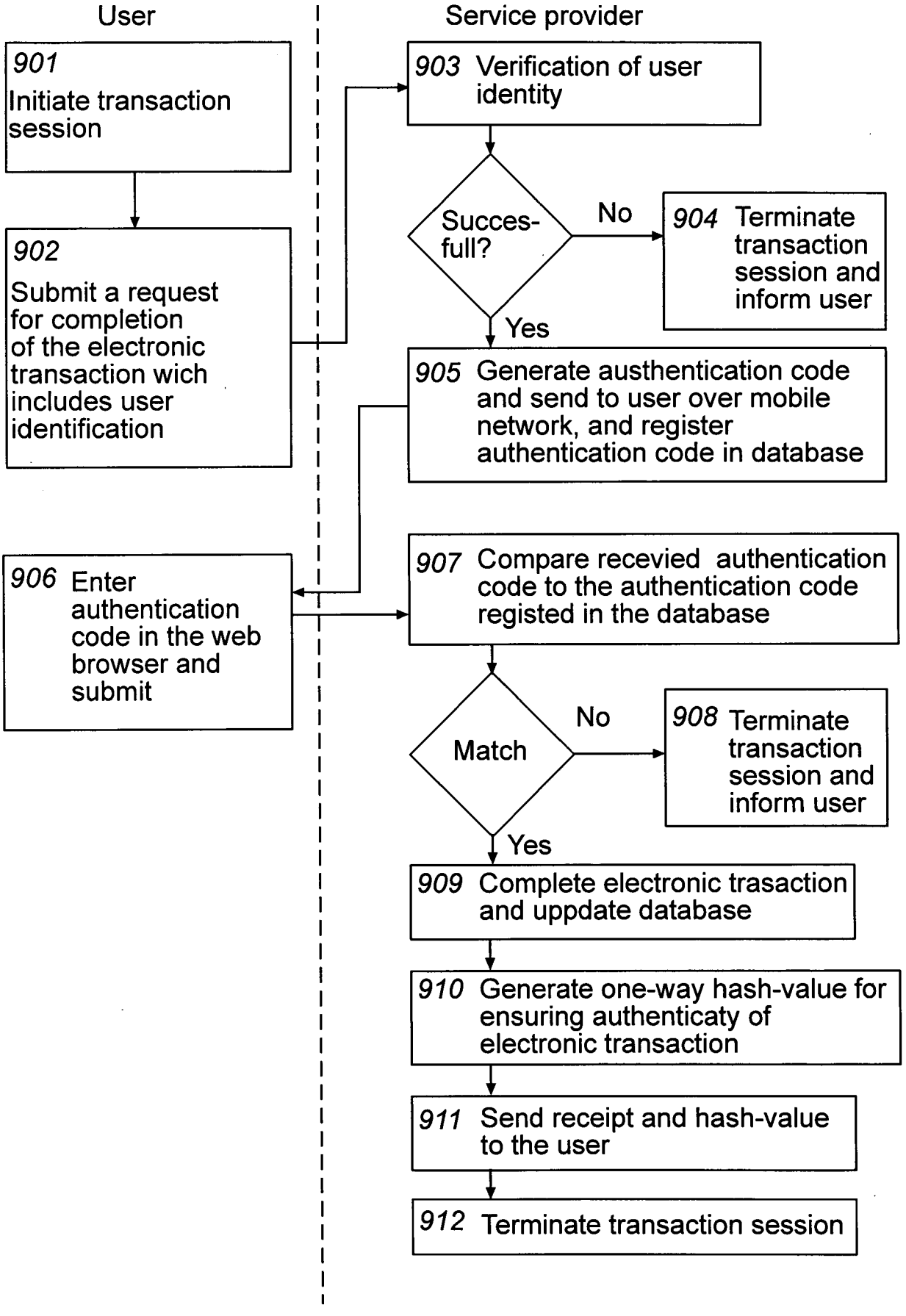

Mobile network
Computer network
Database
Server
Mobile phone
PC
100
200
210
220
300
400
410
420
500

Fig. 1


User
Service provider
901
Initiate transaction session
902
Submit a request for completion of the electronic transaction wich includes user identification
903 Verification of user identity
Succes-full?
No
904 Terminate transaction session and inform user
Yes
905 Generate austhentication code and send to user over mobile network, and register authentication code in database
906 Enter authentication code in the web browser and submit
907 Compare recevied authentication code to the authentication code registed in the database
Match
No
908 Terminate transaction session and inform user
Yes
909 Complete electronic trasaction and uppdate database
910 Generate one-way hash-value for ensuring authenticaty of electronic transaction
911 Send receipt and hash-value to the user
912 Terminate transaction session

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2007/000672

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: G06Q, G06F

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 0221464 A2 (NOKIA CORPORATION), 14 March 2002 (14.03.2002), page 3, line 14 - line 41, figure 1, abstract ---	1-10
Y	WO 9905628 A1 (UNISYS CORPORATION), 4 February 1999 (04.02.1999), figure 6, abstract ---	1-10
A	WO 9944114 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 2 Sept 1999 (02.09.1999) --- --------	1-10

☐ 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 January 2008	25 -01- 2008
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 Oskar Pihlgren/CC Telephone No. +46 8 782 25 00

International patent classification (IPC)
G06Q 20/00 (2006.01)
G06F 21/24 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

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

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.

WO	0221464	A2	14/03/2002	AT	309587	T 15/11/2005
				AU	7763601	A 22/03/2002
				CN	1288607	C 06/12/2006
				CN	1535452	A 06/10/2004
				DE	60114895	D,T 03/08/2006
				EP	1397787	A,B 17/03/2004
				SE	1397787	T3
				EP	1669955	A 14/06/2006
				JP	2004527017	T 02/09/2004
				US	7107248	B 12/09/2006
				US	7308431	B 11/12/2007
				US	20020161723	A 31/10/2002
WO	9905628	A1	04/02/1999	CA	2296602	A,C 04/02/1999
				DE	69808769	D,T 24/07/2003
				EP	0996914	A,B 03/05/2000
				JP	3455179	B 14/10/2003
				JP	3766823	B 19/04/2006
				JP	2001511567	T 14/08/2001
				JP	2003331205	A 21/11/2003
				US	6049786	A 11/04/2000
WO	9944114	A1	02/09/1999	AU	755054	B 05/12/2002
				AU	2831699	A 15/09/1999
				BR	9908246	A 31/10/2000
				CN	1292108	A,T 18/04/2001
				DE	69904570	D,T 15/05/2003
				EE	4444	B 15/02/2005
				EE	200000491	A 15/02/2002
				EP	1058872	A,B 13/12/2000
				FI	980427	A 26/08/1999
				IL	138007	A 25/07/2005
				JP	2002505458	T 19/02/2002
				US	6430407	B 06/08/2002