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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 June 2009 (11.06.2009)

PCT

(10) International Publication Number
WO 2009/071429 A1

(51) International Patent Classification:
G06F 21/20 (2006.01)

(21) International Application Number:
PCT/EP2008/065518

(22) International Filing Date:
14 November 2008 (14.11.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
07122616.1 7 December 2007 (07.12.2007) EP

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **BALTZER, Boris** [DE/DE]; Alte Ziegelei 11, 23866 Nahe (DE).

(74) Agent: **KUISMA, Sirpa (Ms.)**; IBM Deutschland, Management & Business Support GmbH, Patentwesen und Urheberrecht, 70548 Stuttgart (DE).

(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, 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).

Published:
— *with international search report*

(54) **Title:** MOBILE SMARTCARD BASED AUTHENTICATION

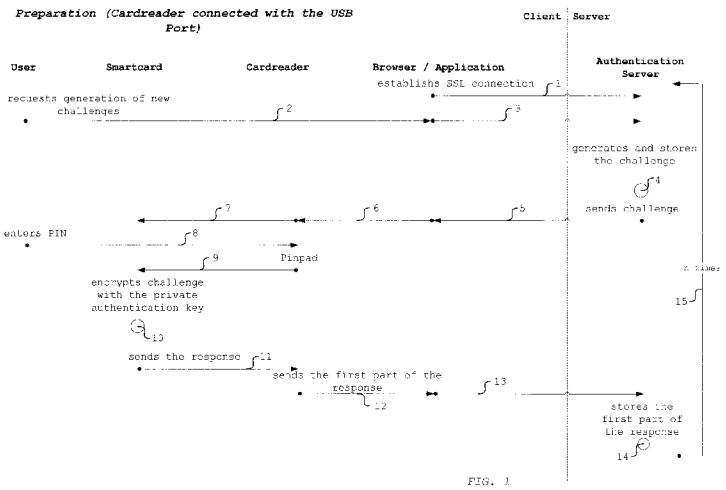

FIG. 1

(57) **Abstract:** In an authentication server, information representing a first part of a response to a challenge is received during the authentication preparation phase. The challenge and the first part of the response are stored for further use. The challenge is resent and information representing a second part of the response to the challenge is received during a modified authentication phase. The first and second parts of the response are checked against the challenge for authenticating the user. In a smartcard reader, the response received from the smartcard is sent to a computing device, when the smartcard reader received the challenge via an interface to the computing device during normal authentication. In response to the smartcard reader having received the challenge via the interface to the computing device during an authentication preparation phase, the smartcard reader sends the first part of the response to the computing device. In response to the smartcard reader having received the challenge via a user interface, it presents at least the second part of the response to a user via the user interface.

WO 2009/071429 A1

D E S C R I P T I O N

Mobile Smartcard Based Authentication

FIELD OF THE INVENTION:
The invention relates to a smartcard reader and an authentication server for processing authentication information as well as to corresponding methods and computer program products for processing authentication information.

BACKGROUND OF THE INVENTION:
The demand for secure user authentication in computer networks, preferably for Internet services, is very high. Passwords are not very secure and might not fulfil the required security standards when personal data, bank accounts or health data have to be protected. Other solutions, like for example electronic tokens, are highly proprietary.

To overcome the problems in security and interoperability, the smartcard technology has been developed, combining standard compliance and very secure algorithms.

The use of smartcards for user authentication is considered to be a strong form of authentication and combines the use of something a user has, i.e. the smartcard, with something the user knows, e.g. a PIN, to provide what is known as two-factor authentication. A smartcard is basically a small plastic card, about the size of a usual credit card, and typically contains a small embedded computer chip, i.e. a microchip, instead of the magnetic stripe provided in traditional credit cards. Smartcards are signature cards. Some of the certificates given on the smartcard are used for signing and some are used for authentication then.

It is known to provide an interactive smartcard login, as well as remote smartcard authentication. Users have the ability to access remote machines via their smartcard and interactively enter the PIN to login, just as if they physically walked up to the console of the remote machine. Remote smartcard authentication and interactive login do not require any type of smartcard middleware, and do not even require a smartcard reader attached to the remote machine.

For above mentioned reasons, smartcards are becoming more and more popular. Officials in several countries are thinking about issuing identity or authentication smartcards for their citizens. Furthermore, banks are issuing an increasing number of cards supporting digital signatures. Smartcards can be used for authentication in Internet services, e.g. in a way where the original issuer of a smartcard takes care of the authentication and then informs a service provider about the outcome of the authentication.

However, there are some problems in using smartcard authentication for services in the Internet. One reason is that most people use more than one computer for their sensitive transactions over the Internet. Therefore a smartcard reader has to be installed for each of the used computers. But even when a smartcard reader and the appropriate software are installed at each computer, a user does not know if the computer can be trusted or if sensitive data on the smartcard will be accessed unwantedly. Commercial certified smartcard readers are only certified for an environment trusted and controlled by the user.

It is an object of the invention to provide secure user

authentication within a computer network, especially for the demand of Internet services. It is a further object of the invention to provide secure user authentication within a computer network, especially when performed on a non-trusted computer of the computer network.

SUMMARY OF THE INVENTION:

The invention provides a method for processing authentication information in a smartcard reader, the method comprising the following steps:

receiving a challenge in the smartcard reader and sending the challenge to a smartcard,

receiving a response to the challenge from the smartcard, said response having at least a first part and a second part,

in response to having received the challenge in the smartcard reader via an interface to a computing device during normal authentication, sending said response to said computing device, in response to having received the challenge in the smartcard reader via an interface to a computing device during an authentication preparation phase, sending the first part of the response to the computing device, and

in response to having received the challenge in the smartcard reader via a user interface of the smartcard reader, presenting at least the second part of the response to a user via the user interface.

When receiving a challenge a smartcard reader will either send a response to a computing device or will send a first part of the response to the computing device or will display a second part of the response. Sending a response to the challenge is the usual case as already having been practised by methods according to the state of the art. Sending a first part of the

response goes together with the computing device having access to the smartcard reader via an interface and is an option provided by a method according to the invention. Sending a second part of the response goes together with the smartcard reader receiving a challenge via an entering process initiated by a user.

The invention further provides a method for processing authentication information in an authentication server, the method comprising the following steps:

sending a challenge during an authentication preparation phase for authenticating a user,

in response to sending the challenge during an authentication preparation phase, receiving information representing a first part of a response to the challenge,

storing the challenge and the first part of the response during the authentication preparation phase for further use during modified authentication,

resending the challenge during modified authentication for authenticating the user,

in response to resending the challenge, receiving information representing a second part of the response to the challenge, and

checking the first and second parts of the response against the challenge and successfully authenticating the user during the modified authentication if the response proves to be valid.

The authentication server either will send a challenge during an authentication preparation phase or will resend the challenge during modified authentication for authenticating the user. There is provided a predefined criterion for triggering the intended authentication step, either

preparation of an authentication in an authentication preparation phase or completing an authentication during modified authentication.

The criterion might be provided by a module either triggering the authentication server to resend a challenge for modified authentication or blocking the authentication server from sending a new challenge for an authentication preparation phase.

The term "computing device" as used with the present invention comprises personal computers, ticket, vending and cash machines, mobile phones and the like and is to be interpreted as broad as possible.

It is an advantage of a method according to the invention that the use of a smartcard with a non-trusted computing device does not provide access to sensitive information at the non-trusted computer, because the smartcard is used without connecting it to the non-trusted computer.

A user can for example be provided with a mobile smartcard reader comprising a keypad and a representing means, preferably a display, for abroad usage, preferably with a rechargeable battery, for use in an Internet Café. A challenge is displayed to the user on a computer screen and the user enters the challenge in the smartcard reader by means of the keypad. The smartcard encrypts the challenge and a second part of the response is displayed on the smartcard reader display. The user enters the second part of the response at the user interface of the computer. The first part of the response has already been stored in the authentication server when the user had performed a "home authentication", i.e. an authentication

with a computing device to be trusted, also called authentication preparation phase.

The term "display" as used with the present invention is to be understood in its broadest sense and comprises all kinds of representing means accessible to a user's sensory perception, e.g. his visual, acoustic and/or haptic perception. Therefore "display a challenge or a response" also comprises audio display via an earphone, for example.

When a user is using the smartcard and a non-trusted computer, the same challenge as with the trusted computer is used again. The user inputs the challenge, preferably of reasonable length, to the smartcard, which calculates the response again. The user is favorably shown a second part of the response which has not been transmitted in the authentication preparation phase with the computing device to be trusted. The user then enters the second part of the response which is transmitted to the authentication server. The authentication server combines the first and second parts of the response and checks whether the combined response is valid.

In the case of a response to a challenge being a sequence of digits, a first part and a second part of the response each are a selection of these digits which may complement one another. "Combining" the first and the second parts of the response then means gaining the complete response.

A user may predefine a mask in an authentication preparation phase which determines the way the selection is made. For example, let the response be a sequence of 40 digits and the mask implement an alternating pattern of the following type: The first part of the response comprises the first, the third,

the fifth etc. digit and the second part of the response comprises the second, the fourth etc. digit. The mask can as well implement another pattern: The first part of the response comprises the first to the thirtieth digit and the second part of the response comprises the thirty-first to the last digit. Actually, there are numerous alternative options. If the second response comprises no more than ten digits an abroad authentication is user-friendly in the sense that only few digits have to be entered in a keypad.

The security of a structure according to the invention relies on two authentication factors: the smartcard and the private authentication key together with the certificates stored on the smartcard. Therefore no proprietary certificates are used, and the authentication server can use any given infrastructure, like directory and revocation services for example, to check the validity of the smartcard and the private authentication key together with the certificates.

The security properties of such a structure are excellent. In case of an unauthorized access to the authentication server the invader will find stored challenges and first parts of responses which do not provide him with the complete information for authentication. If a computing device is attacked during data transmission the invader will only find first or second parts of responses which are useless to him. No relevant data is stored on the smartcard reader itself. If someone watches the user at a computing device, gained information is useless as long as each challenge is used only once.

Therefore each challenge stored in the authentication server is used only once though it is principally possible to use one

challenge several times.

In a preferred embodiment of the method at least one challenge is generated and stored in the authentication server after the step of requesting access to the computer net via a computing device to be trusted.

The term "at least one challenge" comprises the case of generating several challenges in order to maintain a certain supply of challenges. This is advantageous in case a user does not have access to a computing device to be trusted for a while but has to use computing devices not to be trusted for several times. Usually an 8 digit number is sufficient to build a challenge. Every time the user requests an authentication from abroad, i.e. from a non-trusted computing device, the authentication server sends one of the 8 digit numbers.

In a further preferred embodiment of the method after receiving a challenge from the authentication server the challenge is encrypted on the smartcard.

The challenge is favorably encrypted with a private authentication key on the smartcard after entering a PIN in a keypad of the smartcard reader.

The step of checking whether the response is valid favorably comprises the step of decrypting the first and the second parts of the encrypted response and checking them against the challenge.

The first and the second part of the encrypted response are preferably decrypted with the user's public key, i.e. an

asymmetric key design is applied.

In a very practical embodiment of the method the second part of the response comprises a limited number of digits, preferably between 6 and 12 digits, selected from the complete response. In this case it is especially preferred to select the last 6 to 12 digits from the complete response. This restricted number of digits allows a convenient entering by a user. Also the challenge may comprise a limited number of digits, for example between 6 and 12 digits. The number of digits is a compromise between the requirements of security versus the requirements of practicability and comfort.

The method according to the invention is very well suitable to authenticate any user if the first and the second parts of the response are checked against the challenge and the response proves to be valid.

The invention also provides a computer program product containing computer executable instructions for processing authentication information in a smartcard reader and a computer program product containing computer executable instructions for processing authentication information in an authentication server, each of the computer program products corresponding to one of the methods as described above.

The invention further provides a smartcard reader for processing authentication information, the smartcard reader comprising

a user interface component for presenting information to a user and receiving input information from the user;

a first component for providing an interface to a computing device for at least receiving a challenge from the

computing device;

a second component for providing an interface to a smartcard for at least sending a challenge to the smartcard and receiving a response to the challenge from the smartcard, said response having at least a first part and a second part; and

a processing component for controlling operation of the smartcard reader, the processing component causing

the first component to send a response received from the smartcard to said computing device in response to the smartcard reader having received the respective challenge via the interface to the computing device during normal authentication;

the first component to send the first part of a response received from the smartcard to the computing device in response to the smartcard reader having received the respective challenge via the interface to the computing device during an authentication preparation phase; and

the user interface component to present at least the second part of a response received from the smart card via the user interface component in response to the smartcard reader having received the respective challenge via the user interface component.

The invention in addition provides a computing system, for example an authentication server, for processing authentication information, the computing system comprising

means for sending a challenge during an authentication preparation phase for authenticating a user,

means for receiving, in response to sending the

challenge during an authentication preparation phase, information representing a first part of a response to the challenge,

means for storing the challenge and the first part of the response during the authentication preparation phase for further use during modified authentication,

means for resending the challenge during modified authentication for authenticating the user,

means for receiving, in response to resending the challenge, information representing a second part of the response to the challenge, and

means for checking the first and second parts of the response against the challenge and successfully authenticating the user during the modified authentication if the response proves to be valid.

The smartcard reader is adapted to send a first part of a response to a challenge transmitted from the authentication server in a first step and to display a second part of the response to the challenge entered by a user in a second step.

In a preferred embodiment the smartcard reader and the authentication server each are adapted to be used for performing one of the methods as described above.

Examples of smartcards are signature cards from Telesec, Signtrust, TC Trustcenter and D-Trust. Many cards provide a key for authentication and a key for signing documents. Both keys can be used under the algorithm aspect and should be chosen in accordance with the key usage policy of the smartcard.

These, and other, aspects and objects of the present invention

will be better appreciated and understood when considered in conjunction with the following description and the accompanying drawings. It should be understood, however, that the following description, while indicating preferred embodiments of the present invention and numerous specific details thereof, is given by way of illustration and not of limitation. Many changes and modifications may be made within the scope of the present invention without departing from the spirit thereof, and the invention includes all such modifications.

The invention can take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment containing both hardware and software elements. In a preferred embodiment, the invention is implemented in software, which includes but is not limited to firmware, resident software, microcode, etc.

Furthermore, the invention can take the form of a computer program product accessible from a computer-usable or computer-readable medium providing program code for use by or in connection with a computer or any instruction execution system. For the purposes of this description, a computer-usable or computer readable medium can be any apparatus that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device.

The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or a propagation medium. Examples of a computer-readable medium include a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a

random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk and an optical disk. Current examples of optical disks include compact disk - read only memory (CD-ROM), compact disk - read/write (CD-R/W) and DVD.

A data processing system suitable for storing and/or executing program code will include at least one processor coupled directly or indirectly to memory elements through a system bus. The memory elements can include local memory employed during actual execution of the program code, bulk storage, and cache memories which provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage during execution.

Input/output or I/O devices (including but not limited to keyboards, displays, pointing devices, etc.) can be coupled to the system either directly or through intervening I/O controllers.

Network adapters may also be coupled to the system to enable the data processing system to become coupled to other data processing systems or remote printers or storage devices through intervening private or public networks. Modems, cable modem and Ethernet cards are just a few of the currently available types of network adapters.

BRIEF DESCRIPTION OF THE DRAWINGS:
The invention will be better understood from the following detailed description with reference to the drawings, wherein:

FIG. 1 is a diagram illustrating the steps of requesting access to a computer network via a first computing device by connecting a smartcard to the first

computing device by means of a mobile smartcard reader and receiving a challenge from an authentication server and transmitting a first part of a response to the authentication server;

FIG. 2 is a diagram illustrating the steps of requesting access to the computer network via a second computing device and connecting the smartcard to the mobile smartcard reader and receiving a challenge from the authentication server and transferring a second part of a response whereupon the authentication server combines the first and the second parts of the responses and checks whether the response is valid;

FIG. 3 is a schematic illustration of an exemplary environment for the use of the present invention.

FIG. 1 is a diagram illustrating the steps of requesting access to a computer network via a first computing device by connecting a smartcard to the first computing device by means of a mobile smartcard reader and receiving a challenge from an authentication server and transmitting a first part of a response to the authentication server.

The setting is a Client/Server interface indicated by a vertical broken line. The Client runs on the first computing device which is not shown in FIG. 1. The Client side comprises a User, a Smartcard, a Browser/Application and a Cardreader which may be connected to the first computing device via a USB (Universal Serial Bus) Port for data exchange and eventually for loading a battery of the Cardreader, and the Server side

comprises an Authentication Server.

In a first step a SSL (Secure Sockets Layer) connection between the Browser/Application and the Authentication Server is established as indicated by arrow 1. With an SSL connection "man-in-the-middle-attacks" can be avoided, for example.

In a next step the User requests the generation of new challenges. The request is addressed to the Browser/Application as indicated by arrow 2 and transferred to the Authentication Server as indicated by arrow 3. The Application Server thereupon generates and stores one or more challenges 4.

In a further step a challenge 4 is sent to the Cardreader via the Browser/Application as indicated by arrows 5 and 6. The challenge 4 is transferred from the Cardreader to the Smartcard as shown by arrow 7.

The User enters a PIN in a Pinpad of the Cardreader according to arrow 8. The PIN is sent to the Smartcard, see arrow 9. The challenge 4 is encrypted with the User's private authentication key. The encrypted challenge 10, which is called the response, is generated on the Smartcard.

The Smartcard sends the response to the Cardreader according to arrow 11, and from the Cardreader a first part of the response is sent to the Authentication Server via the Browser/Application, see arrows 12 and 13. The first part of the response 14 is stored in the Authentication Server.

The process as illustrated in FIG. 1 can be repeated n times, n being an integer, according to arrow 15, in order to store

first parts of responses 14 for n challenges 4.

The process as described in FIG. 1 can be considered as a preparation process for a process as described in FIG. 2.

The preparation process can be initiated by a user or automatically, for example when a supply of stored unused challenges falls below a certain limit. There can also be provided an automatic routine to remind a user to initiate a preparation process, for example by sending an email message.

It will ease the preparation process if the Smartcard allows an authentication multiple times after the user has entered his PIN.

After a preparation process with a trusted computing device has been performed successfully, the connected smartcard reader can be switched to "abroad authentication" in order to function within a process of authentication with a non-trusted computing device as default case.

FIG. 2 is a diagram illustrating the steps of requesting access to the computer network via a second computing device and connecting the smartcard to the mobile smartcard reader and receiving a challenge from the authentication server and transferring a second part of a response whereupon the authentication server combines the first and the second parts of the responses and checks whether the response is valid.

The setting in FIG. 2 is a Client/Server interface indicated by a vertical broken line as in FIG. 1. The Client runs on the second computing device which is not shown in FIG. 2. The Client side comprises a User, a Smartcard, a Browser and the

Cardreader which is not connected to the second computing device, and the Server side comprises the Authentication Server.

In a first step the User wants to authenticate, see arrow 21, and therefore a SSL (Secure Sockets Layer) connection between the Browser and the Authentication Server is established as indicated by arrow 22.

In a next step the Authentication Server sends a stored challenge 40, which is assumed to be identical to the challenge 4 in FIG. 1, to the Browser as illustrated by arrow 23, and the Browser displays the stored challenge 40 to the User, see arrow 24.

In a further step the User enters the challenge 40 in the Cardreader as indicated by arrow 25, and then the User enters the PIN in the Cardreader as indicated by arrow 26.

The Cardreader sends the challenge 40 to the Smartcard as indicated by arrow 27. The challenge 40 is encrypted with the private authentication key, and the encrypted challenge 20, which is assumed to be identical to the encrypted challenge 10 in FIG. 1, both called the response, is stored on the Smartcard.

The Smartcard sends the response to the Cardreader according to arrow 28, and from the Cardreader a second part of the response is displayed to the User according to arrow 29.

Then the User enters the second part of the response which is sent to the Authentication Server via the Browser, see arrows 30 and 31.

The Authentication Server combines the first and the second parts of the response according to 1.), then decrypts the response with the User's public key according to 2.), then compares the decrypted response and challenge according to 3.). If the decrypted response equals the challenge the User is authenticated according to 4.).

The process as described in FIG. 2 is to be considered as abroad authentication which is based on the preparation process as described in FIG. 1.

FIG. 3 is a schematic illustration of an exemplary environment for the use of the present invention.

A first computing device 300 and a second computing device 400 are connected to a server 500 via a network 600. The first computing device 300 comprises a first user interface 310, a first processor 320 and a first network interface 330. The second computing device 400 comprises a second user interface 410, a second processor 420 and a second network interface 430. The server 500 comprises an authentication server 550. A mobile card reader 700 comprises a pin pad 710 and a display 720 and is adapted to receive a smartcard 800 comprising a microprocessor 850. The microprocessor 850 is adapted to encrypt and decrypt challenges. The mobile card reader 700 can be connected to the first computing device 300 via a USB port 340 as indicated by a broken line. If the first computing device 300 is a computing device to be trusted by a user 900 then a process as described in FIG. 1 is performed. The mobile card reader 700 can be used when working at the second computing device 400 but without being connected to the second computing device 400. If the second computing device 400 is a

computing device not to be trusted by the user 900 then a process as described in FIG. 2 is performed.

It is to be noted that the aspects and embodiments described herein may be conveniently implemented using a machine, e.g. a general purpose computing device, programmed according to the teachings of the present specification, as will be apparent to those skilled in the computer art. Appropriate software coding can readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art.

Such software may be a computer program product that employs a machine-readable medium. A machine-readable medium may be any medium that is capable of storing and/or encoding a sequence of instructions for execution by a machine, e.g. a general purpose computing device, and that causes the machine to perform any one of the methodologies and/or embodiments described herein. Examples of a machine-readable medium include, but are not limited to, a magnetic disk, e.g. a conventional floppy disk, a hard drive disk, an optical disk, e.g. a compact disk "CD", such as a readable, writeable, and/or re-writable CD; a digital video disk "DVD", such as a readable, writeable, and/or rewritable DVD, a magneto-optical disk, a read-only memory "ROM" device, a random access memory "RAM" device, a magnetic card, an optical card, a solid-state memory device, e.g. a flash memory, an EPROM, an EEPROM, and any combinations thereof. A machine-readable medium, as used herein, is intended to include a single medium as well as a collection of physically separate media, such as, for example, a collection of compact disks or one or more hard disk drives in combination with a computer memory.

Examples of a general purpose computing device include, but are not limited to, a computer workstation, a terminal computer, a server computer, a handheld device, e.g. tablet computer, a personal digital assistant "PDA", a mobile telephone etc., a web appliance, a network router, a network switch, a network bridge, any machine capable of executing a sequence of instructions that specify an action to be taken by that machine, and any combinations thereof. In one example, a general purpose computing device may include and/or be included in a kiosk.

While the foregoing has been with reference to particular embodiments of the invention, it will be appreciated by those skilled in the art that changes in these embodiments may be made without departing from the principles and spirit of the invention, the scope of which is defined by the appended claims.

C L A I M S

1. Method for processing authentication information in a smartcard reader, the method comprising the following steps:

receiving a challenge in the smartcard reader and sending the challenge to a smartcard,

receiving a response to the challenge from the smartcard, said response having at least a first part and a second part,

in response to having received the challenge in the smartcard reader via an interface to a computing device during normal authentication, sending said response to said computing device,

in response to having received the challenge in the smartcard reader via an interface to a computing device during an authentication preparation phase, sending the first part of the response to the computing device, and

in response to having received the challenge in the smartcard reader via a user interface of the smartcard reader, presenting at least the second part of the response to a user via the user interface.

2. Method as defined in claim 1, wherein the second part of the response comprises a limited number of digits, preferably between 6 and 12 digits, selected from the complete response.

3. Method as defined in claim 1 or 2, comprising selecting the second part of the response in accordance with a predefined mask.

4. Method as defined in claim 4, comprising negotiating the mask during the authentication preparation phase.

5. Method as defined in any of claims 1 to 4, comprising using cryptography techniques for processing challenges and responses.

6. Computer program product comprising a computer usable medium having computer usable program code for processing authentication information in a smartcard reader, said computer program product including:

computer usable program code for receiving a challenge in the smartcard reader and sending the challenge to a smartcard;

computer usable program code for receiving a response to the challenge from the smartcard, said response having at least a first part and a second part;

computer usable program code for sending said response to said computing device in response to having received the challenge in the smartcard reader via an interface to a computing device during normal authentication;

computer usable program code for sending the first part of the response to the computing device in response to having received the challenge in the smartcard reader via an interface to a computing device during an authentication preparation phase; and

computer usable program code for presenting at least the second part of the response to a user via the user interface in response to having received the challenge in the smartcard reader via a user interface of the smartcard reader.

7. A smartcard reader device comprising:

a user interface component for presenting information to a user and receiving input information from the user;

a first component for providing an interface to a computing device for at least receiving a challenge from the

computing device;

a second component for providing an interface to a smartcard for at least sending a challenge to the smartcard and receiving a response to the challenge from the smartcard, said response having at least a first part and a second part; and

a processing component for controlling operation of the smartcard reader, the processing component causing

the first component to send a response received from the smartcard to said computing device in response to the smartcard reader having received the respective challenge via the interface to the computing device during normal authentication;

the first component to send the first part of a response received from the smartcard to the computing device in response to the smartcard reader having received the respective challenge via the interface to the computing device during an authentication preparation phase; and

the user interface component to present at least the second part of a response received from the smart card via the user interface component in response to the smartcard reader having received the respective challenge via the user interface component.

8. Method for processing authentication information in an authentication server, the method comprising the following steps:

sending a challenge during an authentication preparation phase for authenticating a user,

in response to sending the challenge during an authentication preparation phase, receiving information representing a first part of a response to the challenge,

storing the challenge and the first part of the response during the authentication preparation phase for further use during modified authentication,

resending the challenge during modified authentication for authenticating the user,

in response to resending the challenge, receiving information representing a second part of the response to the challenge, and

checking the first and second parts of the response against the challenge and successfully authenticating the user during the modified authentication if the response proves to be valid.

9. Method as defined in claim 8, comprising generating and storing a set of challenges and a set of first parts of the respective responses during the authentication preparation phase.

10. Method as defined in claim 9, comprising removing challenges from the set of challenges after use during the modified authentication.

11. Method as defined in claim 10, comprising notifying the user when a number of challenges in the set of challenges is below a predefined value.

12. Method as defined in claim 9 or 10, comprising triggering the authentication preparation phase when a number of challenges is below a predefined value.

13. Method as defined in any one of claims 8 to 11, comprising triggering the modified authentication and resending the challenge when a predefined criterion is

fulfilled.

14. Method as defined in claim 13, wherein the predefined criterion is one of the following:

the authentication server is triggered by a module to resend a challenge, and

the authentication server is blocked by a module from sending a new challenge.

15. Method as defined in any one of claims 8 to 14, comprising using cryptography techniques for processing challenges and responses.

16.Method as defined in any one of claims 8 to 15, wherein the second part of the response comprises a limited number of digits, preferably between 6 and 12 digits, selected from the complete response.

17. Method as defined in any one of claims 8 to 16, comprising selecting the second part of the response in accordance with a predefined mask.

18. Method as defined in claim 17, comprising negotiating the mask during the authentication preparation phase.

19. Computer program product comprising a computer usable medium having computer usable program code for processing authentication information in an authentication server, said computer program product including:

computer usable program code for sending a challenge during an authentication preparation phase for authenticating a user,

computer usable program code for receiving, in

response to sending the challenge during an authentication preparation phase, information representing a first part of a response to the challenge,

computer usable program code for storing the challenge and the first part of the response during the authentication preparation phase for further use during modified authentication,

computer usable program code for resending the challenge during modified authentication for authenticating the user,

computer usable program code for receiving, in response to resending the challenge, information representing a second part of the response to the challenge, and

computer usable program code for checking the first and second parts of the response against the challenge and successfully authenticating the user during the modified authentication if the response proves to be valid.

20. Computing system for processing information,said computing system comprising

means for sending a challenge during an authentication preparation phase for authenticating a user,

means for receiving, in response to sending the challenge during an authentication preparation phase, information representing a first part of a response to the challenge,

means for storing the challenge and the first part of the response during the authentication preparation phase for further use during modified authentication,

means for resending the challenge during modified

authentication for authenticating the user,

means for receiving, in response to resending the challenge, information representing a second part of the response to the challenge, and

means for checking the first and second parts of the response against the challenge and successfully authenticating the user during the modified authentication if the response proves to be valid.

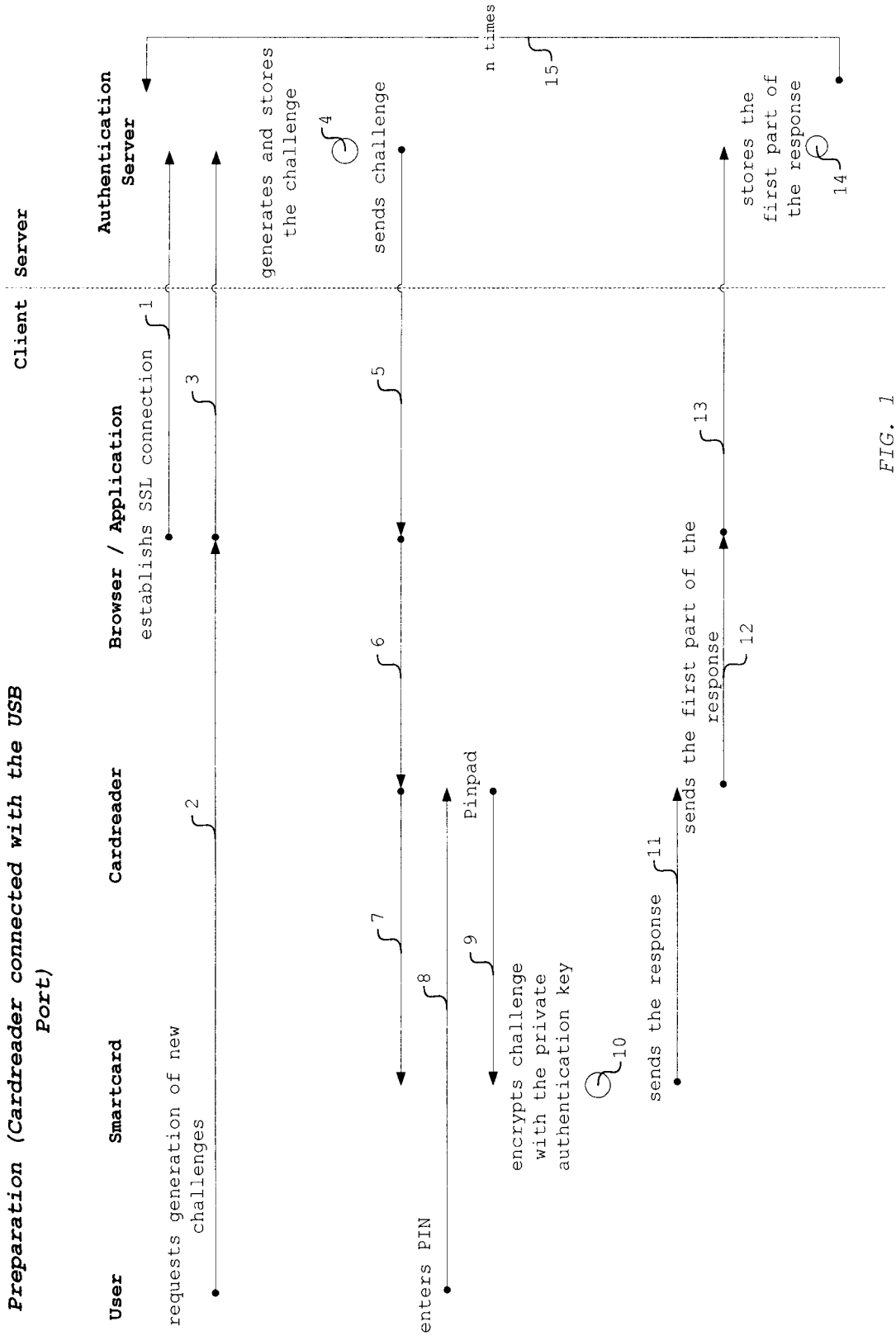
Preparation (Cardreader connected with the USB Port)
Client
Server
User
Smartcard
Cardreader
Browser / Application
Authentication Server
establishs SSL connection
1
requests generation of new challenges
2
3
generates and stores the challenge
4
sends challenge
5
6
7
enters PIN
8
Pinpad
9
encrypts challenge with the private authentication key
10
sends the response
11
sends the first part of the response
12
13
stores the first part of the response
14
n times
15

FIG. 1

FIG.1

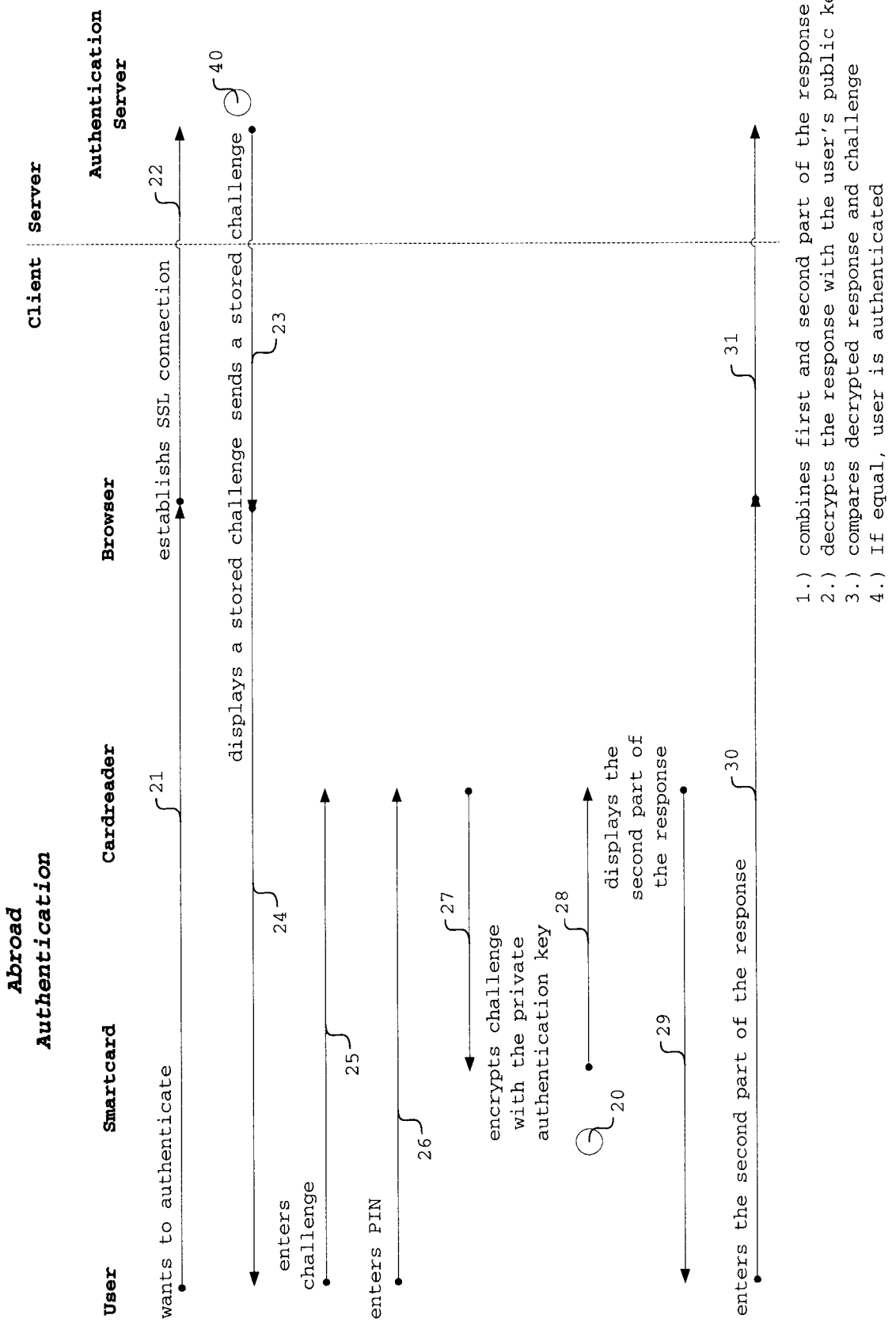
Abroad Authentication
User
Smartcard
Cardreader
Browser
Client
Server
Authentication Server
wants to authenticate
21
establishs SSL connection
22
displays a stored challenge
40
displays a stored challenge sends a stored challenge
23
enters challenge
24
enters PIN
25
26
encrypts challenge with the private authentication key
27
20
displays the second part of the response
28
29
enters the second part of the response
30
31
1.) combines first and second part of the response
2.) decrypts the response with the user's public key
3.) compares decrypted response and challenge
4.) If equal, user is authenticated

FIG. 2

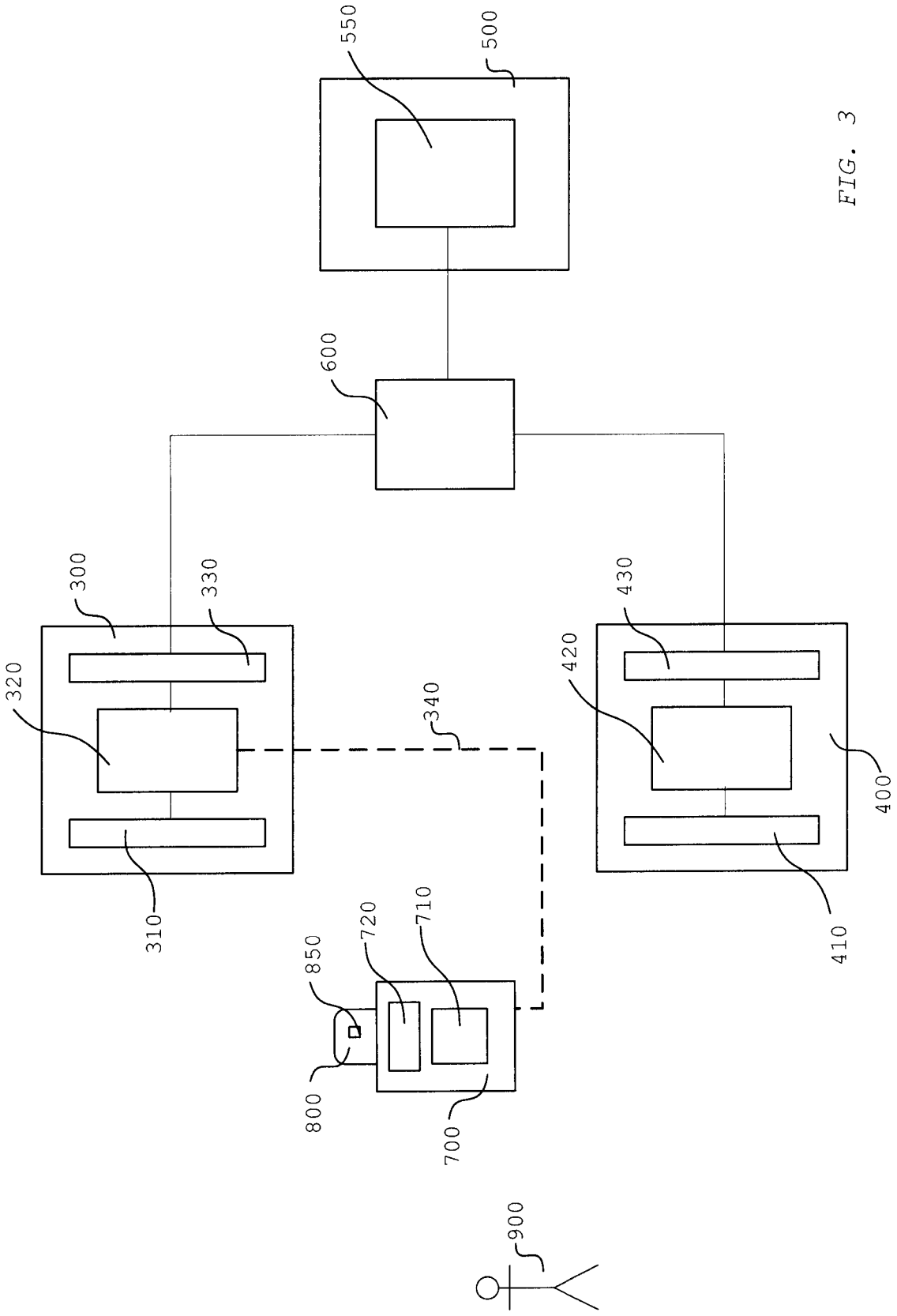
550
500
600
300
330
320
340
430
420
400
310
410
850
720
710
800
700
900

FIG. 3

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/065518

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/20

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)
G06F G07F H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 94/00936 A (LANG GERALD [US]) 6 January 1994 (1994-01-06) page 4, line 21 - page 5, line 10 page 10, line 1 - page 14, line 16 figures 1,2	1-7
X	WO 2007/104923 A (BRITISH TELECOMM [GB]; COFTA PIOTR LEON [GB]) 20 September 2007 (2007-09-20) page 7, line 14 - page 11, line 19 page 20, column 21 - column 33 page 21, line 21 - line 30	8-20
X	US 6 549 912 B1 (CHEN ANN-PIN [US]) 15 April 2003 (2003-04-15) column 18, line 15 - column 19, line 38 figure 9	8,15,19, 20

☐ 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 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
20 January 2009	27/01/2009

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	Segura, Gustavo

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/065518

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9400936 A	06-01-1994	NONE	
WO 2007104923 A	20-09-2007	CA 2644772 A1	20-09-2007
		EP 2014046 A1	14-01-2009
		US 2009011739 A1	08-01-2009
US 6549912 B1	15-04-2003	AU 774434 B2	24-06-2004
		AU 1091900 A	10-04-2000
		AU 2004214511 A1	14-10-2004
		CA 2345391 A1	30-03-2000
		EP 1116151 A2	18-07-2001
		WO 0017794 A2	30-03-2000