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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11575 A1

(51) International Patent Classification[7]: G07F 7/10

(21) International Application Number: PCT/BE00/00092

(22) International Filing Date: 2 August 2000 (02.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/369,925 9 August 1999 (09.08.1999) US

(71) Applicant: **WOW COMPANY S.A.** [BE/BE]; Rue du Coquelet 18, B-5000 Namur (BE).

(72) Inventors: **GILLIARD, Jean-Marc**; Rue Haie des Chats 8, B-6500 Renlies (BE). **DEMARTEAU, Joseph**; Rue de Coquelet 18, B-5000 Namur (BE).

(74) Agents: **POWIS DE TENBOSSCHE, Roland** et al.; Cabinet bede S.A., Place de l'Alma 3, B-1200 Brussels (BE).

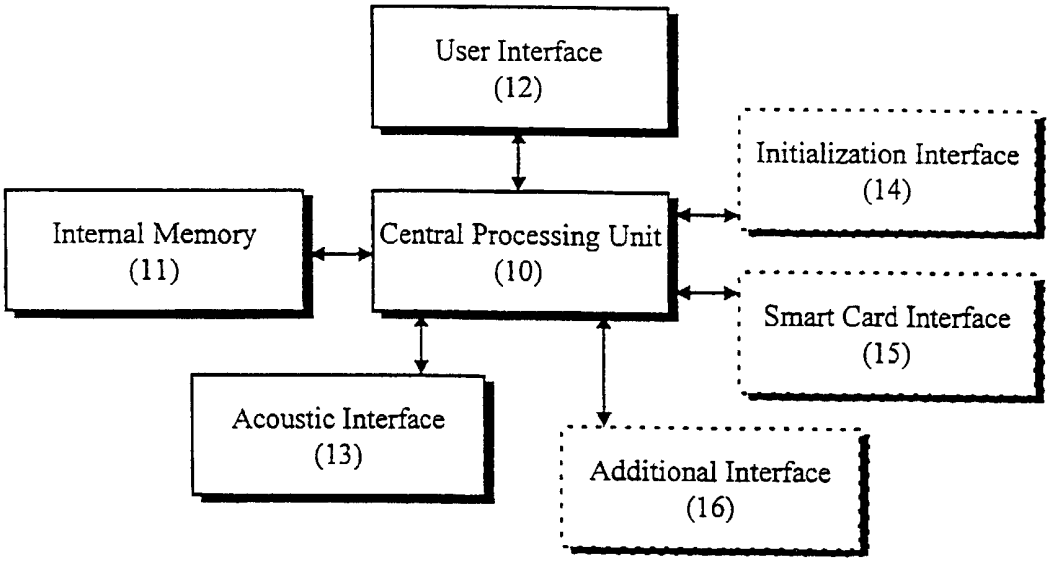
(81) Designated States *(national)*: CA, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

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.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PORTABLE CERTIFICATION DEVICE WITH ACOUSTIC COUPLING



(57) Abstract: A portable certification device comprises a compact housing provided with: data storage means for storage of at least one cryptographic key and/or smart card interface; processing means for computer processing; at least one acoustic interface for wireless exchange of information with the device, by means of at least an acoustic signal generated using a modulation technique selected from the group consisting of: frequency-shift keying, phase-shift keying, amplitude-shift keying and any combination thereof; means for supplying power to the acoustic interface, processing means, storage means and/or smart card interface.

WO 01/11575 A1

PORTABLE CERTIFICATION DEVICE WITH ACOUSTIC COUPLING

Field of the invention

The invention relates to certification methods and, more particularly, to user and data authentication and encryption systems.

Background of the invention

The increasing demand for information transfer over various networks, including PSTN (public switched telephone network) and the Internet, makes necessary that security tools are used to protect sensitive data and/or to restrict remote access to a resource (e.g.: sensitive file, database server, etc.) to authorized persons only. Some of these tools consist of a kind of pocket calculator with cryptographic capabilities; they are known as "security tokens".

Generally, security tokens generate codes ("digital signatures") which are used to certify remote transactions. To achieve a high security level, a user's PIN (personal identification number) must be entered into most security tokens before they can generate valid authentication codes. This is known as a two-factor security scheme; valid codes can be generated only when two things are used simultaneously: something the user possesses (the token) and something the user knows (the PIN).

Compared to other cryptographic tools, the security tokens offer the advantage of being portable and compatible with various commutation media. The main problem encountered with such devices is the difficulty to interface them with another terminal for automatic data interchange. Actually, data to authenticate is generally input manually by the user through the keypad of the token, and the user has to enter the output data displayed by the token (usually the authentication codes) into the communication terminal. Some solutions have already been investigated to make this data transfer more user-friendly.

As an example, some security tokens are dedicated to authentication of transactions made by means of personal computer ("P.C."). They allow automatic input of data by infrared interface (using a dedicated P.C. peripheral) or by optical reading on the P.C. screen. Other tokens, rather dedicated to phone transactions, use the standard DTMF (dual tone multi-frequency) signals to output the generated codes either through an electrical connection or through a speaker or buzzer. In this latter case, the tokens can be considered as the well known DTMF dialers, equipped with cryptographic capabilities.

On the other hand, FSK (frequency-shift keying) and other modulation techniques have been widely used for bi-directional acoustic coupling of low transmission speed modems. Most of these modems are now obsolete because of the requirements for high speed data transfers.

The present invention combines the technologies of security tokens and acoustic modulation techniques, so as to provide a powerful security tool, efficient and easy to use, compatible with almost any communication media, thanks to its wireless acoustic interface.

Brief description of the invention

The present invention is a portable certification device ("PCD"), capable of receiving and/or transmitting data through a wireless acoustic interface. Certification is herein defined as a technique to restrict remote access to a resource to authorized persons only and/or to protect sensitive data during the transmission. Data protection may include data authentication (or electronic signature), for example to ensure that said data have not been modified during transmission, and/or data encryption to prevent unauthorized access to the said data.

The portable certification device of this invention comprises a compact housing provided at least with:

a. first means selected from the group consisting of :

- data storage means for storage of at least one cryptographic key;
- a means for at least reading information from a smart card containing at least one cryptographic key ;
- any combination thereof ;

b. at least one acoustic interface for wireless exchange of information with the device, by means of at least an acoustic signal generated using a modulation technique selected from the group consisting of: frequency-shift keying, phase-shift keying, amplitude-shift keying and any combination thereof;

c. processing means, at least for processing signal between the acoustic interface and said processing means;

d. means for supplying power to the first means, processing means and acoustic interface.

The preferred modulation technique is frequency-shift keying.

Advantageously, the processing means process at least a signal by means of an algorithm using at least one cryptographic key.

At least one acoustic interface can be used to input data to be processed by the processing means and/or to output data processed by the processing means. The same or different interface and/or modulation technique can be used to input and output data.

According to one embodiment, the device is equipped with a smart card interface, for smart card data interchange.

In another embodiment, the device is further provided with a at least one non-acoustic interface for data interchange.

According to a detail of a device of the invention, the processing means comprise an algorithm selected from the group consisting of : algorithm for unique user identification, algorithm for data authentication, algorithm for data encryption, and any combination thereof, and/or the device comprises a means for at least reading information from a smart card, the said smart card comprising an algorithm selected from the group consisting of : algorithm for unique user identification, algorithm for data authentication, algorithm for data encryption, and any combination thereof. For example, the processing means comprise a first algorithm selected from the group consisting of : algorithm for unique user identification, algorithm for data authentication, algorithm for data encryption, and any combination thereof, while the said device further comprises a means for at least reading information from a smart card, the said smart card comprising a second algorithm selected from the group consisting of : algorithm for unique user identification, algorithm for data authentication, algorithm for data encryption, and any combination thereof ; the said second algorithm being different from the first.

According to a characteristic of an embodiment, the device comprises data storage means for at least one cryptographic key and/or a means for at least reading information from a smart card containing at least one cryptographic key. For example, the device comprises data storage means for at least a first cryptographic key and a means for at least reading information from a smart card containing at least a second cryptographic key, different from the first one.

For specific use, the device may comprise initialization means. For example, the said initialization means include radio signal reception means.

According to another characteristic of an embodiment, the device further comprises user interface means, allowing control of the device. For example, the said user interface means include at least a keypad and/or at least on/off switching means and/or a user display.

The acoustic interface may comprise at least a microphone and/or a speaker and/or buzzer and/or any combination thereof. In a preferred embodiment, the speaker is used as bi-directional acoustic interface.

As a result of the present invention, a portable security device is provided which can be interfaced to various communication media by means of wireless acoustic coupling. This device can be used as an access control means and/or user or data authentication and/or encryption tool. Although the present invention has been preliminary designed for remote certification, other applications can easily be considered by those skilled in the art.

The invention relates also to a certification method having the improvement of exchanging data by means of at least an acoustic signal generated using a modulation technique selected from the group consisting of: FSK (frequency-shift keying), PSK (phase-shift keying), ASK (amplitude-shift keying) and any combination thereof.

The method can be applied for access control and/or user authentication and/or remote transaction certification and/or data authentication and/or data encryption.

Processing means of the PCD are used preferably to generate unpredictable digital signatures for user and/or data authentication. It is to be appreciated that either symmetrical (private key) or asymmetrical (public key) encryption algorithm can be implemented in the PCD for digital signature generation.

The PCD will preferably comprise a keypad to enter the user's PIN (personal identification number); the said PIN being required by the processing unit for generation of valid digital signatures. In a preferred embodiment of this invention, this PIN will never be stored in the PCD, nor transmitted on the communication

channel. In another embodiment, when a lower security level is acceptable for the application, the PCD will operate without the need of user's PIN entry. In this latter case, no keypad is provided on the PCD, but a single on/off switch will be used; when powered on, the PCD will automatically generate an authentication code and send it through the acoustic interface.

The PCD will also preferably comprise a display for user guidance and for displaying generated authentication codes or other information. In a preferred embodiment, user guidance will be achieved by means of symbols on the display.

As a result of the present invention, a portable security device is provided which can be interfaced to various communication media by means of wireless acoustic coupling. This device can be used as an access control means and/or data authentication and/or encryption tool. Although the present invention has been preliminary designed for remote certification, other applications can easily be considered by those skilled in the art.

Preferred embodiments of the invention will be described in greater details below. This description should be considered as an illustration, but it is not intended to restrict in any way the scope of the present invention.

Brief description of the drawings

Fig. 1 is a block diagram of a preferred functional description of the invention.

Fig. 2A, 2B and 2C are respectively a front view, side view and rear view of a physical embodiment of the invention.

Fig. 3 depicts a preferred embodiment of the authentication algorithm.

Fig. 4 describes a typical operating environment of the invention.

Fig.5 depicts another configuration of the server modules of Fig. 4.

Fig.6 depicts a possible configuration of the acoustic interface.

Fig.7 shows another possible configuration of the acoustic interface.

Fig.8 depicts still another possible configuration of the acoustic interface.

Fig.9 shows an improved version of the configuration depicted by Fig.8.

Detailed description of preferred embodiments

The present invention is a portable certification device, hereinafter referred to as "PCD", equipped with wireless acoustic coupling interface. It can be used as a security token for user and/or data authentication and/or for data encryption.

A functional description of the PCD is shown in Fig. 1. It is to be appreciated that this functional block diagram does not necessarily describe the physical implementation of the invention. Actually, several functions can be integrated into the same physical component; alternatively, some functions can be implemented by means of several components. Moreover, all these functional modules are interconnected through microprocessor bus and/or electronic circuits which will not be described in the scope of this document, as this technology is rather trivial for those skilled in the art. Similarly, a battery and/or any other power supply module and/or circuitry are considered as obvious components of the PCD which will not be described here, because a large variety of such modules are well known in the art.

It is to be understood that Fig. 1 depicts a preferred functional description of the invention, but variations are possible by selectively excluding or including certain

functional modules, depending on the application. According to Fig. 1, the PCD preferably includes a central processing unit (10) with its internal memory (11) (e.g.: RAM, ROM, EEPROM, etc.), a user interface (12) and an acoustic interface (13). Optionally, a dedicated initialization interface (14) and/or a smart card interface (15) can also be provided. Furthermore, an additional interface (16) may be included for specific applications. The arrows depicts the exchange of signals between the central processing unit (10) and the other peripherals (11), (12), (13), (14), (15), and/or (16).

It is obvious for those skilled in the art that a one-chip microprocessor may include the central processing unit (10) and the internal memory (11). The application software is preferably stored in the microprocessor ROM (read only memory) during production of the chip (masked microprocessor), while specific parameters (encryption keys, device serial number, etc.) are preferably stored into the microprocessor RAM (random access memory) during a device initialization procedure. The user interface (12) is used by the user for controlling the device. Fig.2 depicts an example where this user interface physically consists of a keypad and a display, with their associated circuitry for communication with the microprocessor.

The acoustic interface (13) allows wireless coupling of the PCD to various communication channels. This interface will be described with more details later.

The initialization process, also described later in more details, may use the acoustic interface (13), or even the user interface (12) for information transfer. However, in a preferred embodiment, a specific initialization interface (14) is provided. According to a possible improvement of the device, this interface may include a short-distance radio transmission channel, in such a way that no mechanical operation is required on the device (not even pressing the "on" key) to trigger the initialization process in the device.

According to a possible improvement of the device, the PCD may include an integrated smart card interface (15). Such interface for connection between a smart card and a microprocessor is well known by those skilled in the art and will not be described here. With such interface, the cryptographic data and/or processing of the PCD can be partially or completely located on a smart card.

According to a further possible improvement of the device, an additional interface (16) is included to enhance the capabilities of the PCD. By way of example, this additional interface may be used for connecting an external power supply module or for exchanging data by another means than the acoustic coupling.

A preferred physical embodiment of the invention is illustrated in Fig. 2. Referring to this figure, a front- , bottom- and side-view of a preferred design of the housing (20) are depicted. Shape and dimensions of this preferred housing have been designed for easy operation of the device, even with one hand only, and for easy interface to a telephone handset or a personal computer. A keypad (21) similar as a telephone keypad is provided for digits and "*" and " #" symbols entry, the letters printed on these keys can be used for mnemonic remembering of the PIN. As an option of one embodiment of the invention, a fully alphanumeric keypad can be provided for alphanumeric data entry, when required for the application. At least one other key (22) is provided for triggering of the acoustic signal transmission and/or detection. One or more keys (23) are powering the device on and off ; these keys will preferably be protected to avoid unexpected power-on of the device, for example when it is stored in a pocket. Such protection may consist in a ring (24) surrounding the said on/off key(s). The display (25) is preferably a liquid crystal display matrix; it is used for user guidance and/or for displaying generated authentication codes and/or other information. In this preferred embodiments, holes (26) are provided on the bottom side of the housing (20) to ensure efficient acoustic coupling of the PCD with various types of communication terminals.

It is to be appreciated that the Fig. 2 is given as an illustration of a possible embodiment of the application and should not be construed as a restrictive description of the invention. By way of example, the keypad (21) needs not to be present for applications where user's PIN entry is not required, another embodiment could be designed without display (25), still another embodiment could use a flexible membrane instead of holes (26), in order to allow acoustic coupling while being waterproof, etc.. Furthermore, it is to be noted that the PCD may also be physically protected against tampering, by means of one of the various techniques well known by those skilled in the art.

Fig. 3 depicts one embodiment of the authentication algorithm. Depending on the application, the cryptographic algorithm CRYPTO (305) may be either a symmetrical (private key) or an asymmetrical (public key) encryption algorithm ; many existing standards (D.E.S., R.S.A., etc.) are well known by those skilled in the art. Depending on the chosen cryptographic algorithm CRYPTO (305), one or more cryptographic keys are needed; in the following description, the KEY (304) parameter may therefore designate one or more encryption keys.

In the preferred embodiment depicted by Fig. 3, it is assumed that during an initialization process (explained later), the encryption key(s) have been stored in the device memory (11 of Fig. 1) in an encoded form SKEY (303), so that user's PIN (301) is required for decoding. Various techniques for such encoding are well known in the art. Accordingly, the PIN (301) entered by the user is input to the P_FMT function (302) which decodes SKEY (303), in order to retrieve the encryption key(s) KEY (304) to use with the selected cryptographic algorithm CRYPTO (305). It is worth noting that the technique used in this embodiment makes the PIN indispensable for valid authentication, although this PIN is never stored in the device nor transmitted on the communication channel.

It should be noted that in another embodiment of the invention, SKEY (303) may be either partially or totally stored on a smart, card which can be accessed by means of the smart card interface (15 of Fig. 1). In still another embodiment, the cryptographic algorithm CRYPTO (305) may also be partially or totally located on a smart card. For example, in this latter case, the processing means of the device need not to include cryptographic means and the complete device may be considered as a smart card interface, to be used with various communication terminals, including P.C. and telephone.

Furthermore, it is to be appreciated that in embodiment requiring a lower security level, no PIN needs to be entered. In this case, the authentication algorithm depicted by Fig. 3 is still valid, but items 301, 302 and 303 have to be removed. In this embodiment, when the device is activated by the user (preferably by means of a single on/off key), the parameter KEY (304) is retrieved from device memory and/or from a smart card, for execution of the authentication process.

For user authentication, the parameters PARAM (306) entered as data fields to the cryptographic algorithm CRYPTO (305) preferably consists in an initialization vector (preferably filled with zeroes), followed by the device serial number and a sequential number incremented before each new authentication code generation. The data authentication algorithm is preferably similar as user authentication algorithm, except that not only the parameters PARAM (306), but also the data fields DATA (307) are input to the cryptographic algorithm CRYPTO (305). In a preferred embodiment of the invention, the worldwide standard D.E.S. (Data Encryption Standard) is used in CBC (cipher block chaining) mode; this technology is well known by those skilled in the art.

The resulting output of CRYPTO (305) is preferably passed to a formatting function C_FMT (308) which manipulates its input in order to output an authentication code complying with the format specified for the application. In one

embodiment of the invention, this C_FMT (308) function combines the left and right parts of the 16 hexadecimal digit output of the D.E.S., chosen as CRYPTO algorithm (305), in order to provide a 8 hexadecimal digit number which is further converted into a 8 decimal digit authentication code. The output of C_FMT (308) is passed to the message formatting function M_FMT (311) which builds the authentication message M_OUT (312) according to the format specified for the application. In a preferred embodiment of the invention, the authentication message M_OUT (312) consists of the device serial number, a part of the current value of the sequential number incremented for each code generation, the resulting authentication code and a CRC (cyclic redundancy checksum) for detection of eventual transmission errors.

In another embodiment of the invention, the message M_OUT (312) also includes the data to be authenticated. If no encryption is required by the application, the said data will be included in clear text (i.e. without encryption) in the message and the authentication code will ensure that data are not modified during transmission. For applications requiring confidentiality of the transmission, only encrypted data are included in the message M_OUT (312). In this latter case, the CRYPTO algorithm (305) is used not only to generate an authentication code, but to provide a complete encrypted message which can be decoded after transmission so as to retrieve the original data message. Various methods for such encryption are well known in the art.

In a particular embodiment of the invention, a PIN check value P_CHK (310) can be stored in the device memory (11 of Fig. 1) so that the validity of the PIN (301) entered by the user on the device keypad can be checked before generation of an authentication code. For that purpose, the P_CHK value (310) is generated during the initialization process (described later) by running the CRYPTO algorithm (305) using the encryption key(s) KEY (304) and predefined fixed value of parameter PARAM (306); the resulting output is formatted by the C_FMT function (308),

then preferably partially extracted by the P_EXT function (309) and stored in the P_CHK value (310). The P_EXT function (309) is provided so that the output of C_FMT (309) may be partially or completely stored in P_CHK value (310), depending on application requirements. When the user's PIN (301) is entered on the device keypad, the KEY value (304) is retrieved by means of the P_FMT function (302) and the CRYPTO algorithm (305) is run using the said predefined fixed value of parameter PARAM (306); the resulting output is converted by the C_FMT (308) and P_EXT (309) functions and finally compared to the previously stored value of P_CHK (310). If both values do not match, the PIN entry is rejected. In a preferred embodiment, the device is locked when successive unsuccessful attempts for PIN entry are detected, to prevent fraudulent use of the device by unauthorized persons. The said locking can be either temporary or permanent and preferably consists in disabling all functions of the device, making it not operational for the duration of the locking period.

In a preferred embodiment of this invention, all devices are identical just after their production. Consequently, before it can be used, each device has to be personalized by means of the initialization process. This process preferably consists in transmitting parameters specific to each device for storage in the device memory. In a preferred embodiment, these parameters are: the device serial number, initial value for sequential number to be incremented for each transaction, encryption key(s) and various flags for selection of operating options. The initialization process is preferably achieved by means of an initialization machine; a preferred embodiment of such machine consists in a computer (e.g. a P.C.) linked to its peripherals, preferably including a printer and a dedicated interface for communication with each PCD to initialize.

In a particular embodiment, this initialization process can be triggered in the device by means of short-distance radio transmission. Considering that each device is preferably coming from the production factory packed in an individual box and

with its microprocessor unit waiting in stand-by mode, the short-distance radio transmission allows to "awake" the microprocessor (so that it will enter the initialization process) without need to open the individual packing box. Once this initialization process has been triggered, communication is successively established between each PCD to initialize and the initialization machine. In a preferred embodiment, this communication uses the short-distance radio transmission to send data from the initialization machine to the PCD and the acoustic interface to send acknowledgement data from the PCD to the initialization machine. However other embodiments could use any kind of communication media for data exchange between the PCD and the initialization machine, eventually including a specific initialization interface in the PCD.

The initialization process preferably comprises two steps: the transmission of specific parameters (e.g.: serial number, encryption key(s), etc.) from the initialization machine to the PCD and the transmission of an acknowledgment signal from the PCD to the initialization machine, when the procedure has been successful. In a preferred embodiment, once this acknowledgment has been received, the initialization machine can print a label to be put on the PCD box for identification (the said label giving, for instance, the device serial number and the date of initialization) and store the initialization data in a secured database to be transferred to the authentication server (described later).

It is to be appreciated that, in some embodiments of this invention, the initialization process transfers to the PCD multiple sets of parameters, each set corresponding to a specific authentication server. Accordingly, the same PCD can be used to authenticate transactions with various applications which can either share or not the same authentication server. It should also be noted that multiple set of parameters need not necessarily to be initialized at the same time. Actually, some embodiments of the invention allow remote updating of PCD parameters by

means of a predefined secure procedure, using for example the acoustic interface for encrypted data transfer.

Fig. 4 depicts a typical operating environment of the invention. It is to be appreciated that the present invention can be used in a wide range of various environments which may significantly differ from the one depicted in Fig. 4. The following description of the PCD operations in this environment can easily be transposed for other environments. Furthermore, it should be noted that the specificity of the present invention resides in the use of a portable device acoustically coupled to whatever terminal; the rest of the authentication process described hereinafter, including the way data are processed by the authentication server, is not restricted to the use of the present invention, such process is common to most security environments and is well known in the art.

A user (41) is willing to communicate with an application server (45), by means of a communication network (44) and a communication terminal (43) connected to the said communication network and preferably equipped with an acoustic interface for communication with the user's PCD (42). This acoustic interface of the terminal (43) preferably consists in a microphone and a speaker or buzzer. Acoustic coupling between the PCD and the terminal is simply achieved by placing the PCD in the vicinity of the said acoustic interface of the terminal. As a way of example, the terminal (43) can be a telephone with the handset being the acoustic interface or else it can be a P.C. equipped with peripherals including a microphone and a speaker and/or buzzer.

In order to prevent unauthorized access to the application server (45), an authentication server (46) is provided, which is connected to the application server (45) either through the said communication channel (44), or via another connection, or both. In a preferred embodiment of the application, the authentication server (46) may be used as a "front-end" or "firewall" system for the application server (45), as

depicted in Fig. 5. The security protocol of the authentication server (46) preferably requires use of PCD (42) for each authorized user, who has received such a PCD (42) duly initialized. The initialization database of all PCD's distributed to authorized users has been securely transferred to the authentication server (46), from the initialization machine. The procedure for such database transfer will not be described here, as many various secure procedures are well known in the art for this kind of transmission.

In a preferred operating mode of the present invention, when the user (41) wants to establish a communication with the application server (45), he or she uses the terminal (43) to connect to the application server (45). The authentication server (46) is alerted either by the application server (45) or, in the configuration depicted in Fig. 5, even before any access is made to the application server (45). The said authentication server (46) prompts the user (41) for logging. The user (41) powers on his or her PCD (42) and is prompted for PIN entry, preferably by means of symbols on the display of the PCD (42). The user's PIN is entered by means of the PCD keypad (21 of Fig. 2). In a preferred embodiment, the PIN is checked by the PCD by means of the P_CHK code (310 of Fig. 3) and a positive or negative acknowledge is displayed on the PCD display, preferably by means of symbols. If the PIN is valid, an authentication code can be generated (and preferably displayed on the PCD display) and an authentication message (312 of Fig. 3) is built. The PCD (42) is placed by the user (41) in the vicinity of the acoustic interface of the terminal (43), and the user (41) can start the acoustic transmission of the said authentication message, preferably by pressing the transmission key (22 of Fig. 2) on the PCD keypad. In a preferred embodiment of the invention, the acoustic signal is generated using the FSK (frequency-shift keying) encoding technique, but other possibilities for such generation are well known in the art.

As previously mentioned, the said acoustic signal transmitted to the terminal (43) comprises in encoded form (preferably FSK) several data fields, preferably

including the PCD serial number, the authentication code and part of the current value of the sequential number to be incremented for each authentication code generation. This information is received by the terminal (43), which sends it through the communication network (44) to the authentication server (46). The received device serial number allows the authentication server to retrieve from its database the information concerning this device, including the encryption key(s); the received partial value of sequential number is used to synchronize the information from the database and the authentication algorithm (depicted by Fig. 3) is run for validation of the received authentication code. If this code is valid, a positive acknowledgement can be sent to the application server (45) and the user (41) is allowed to enter the application session.

The PCD (42) can also be used for data authentication or encryption. In a preferred embodiment, the procedure is similar as for user authentication, except that after user's PIN entry, data to authenticate or to encrypt are also entered in the PCD. This data entry can be done either manually by means of the device keypad (21 of Fig. 2) or automatically by means of the wireless acoustic connection with the terminal (43), or else by means of an additional interface (16 of Fig. 1). In a similar way, a secure communication can be established between the PCD (42) and the authentication server (46) or an initialization machine connected to the communication network (44) for remote updating of the internal parameters of the PCD (42).

In a preferred embodiment of the invention, when data fields to be authenticated or encrypted have been introduced in the device (either manually via the keypad or automatically via the acoustic interface or additional interface), the user has the opportunity of visualizing the said data fields on the display of the PCD for validation before generation of the authentication code and/or encrypted message.

Fig. 6 depicts an embodiment of the acoustic interface. In this particular embodiment, the acoustic interface is used only to output data processed by the processing unit (10). This data is first converted in an analog signal and modulated by the modulation module (60). Various techniques for such digital to analog conversion are well know in the art and they will not be described here. The acoustic signal is output from the device to a terminal (43) by means of a speaker (61), but a buzzer could also be used in another embodiment. The terminal (43) is equipped with a microphone to receive the said acoustic signal. If, for example, this terminal is an analog telephone, the said acoustic signal is transmitted trough the communication network (44 of Fig. 4) and will be decoded by the authentication server and/or the application server. In another example, where the terminal is a P.C. equipped with a microphone and a sound processing card , the received acoustic signal is preferably demodulated by the P.C. and converted back into a digital signal, to be sent on the communication network using the same protocol as for other data exchanged between the terminal and the application server. Accordingly, a demodulator and analog to digital converter must be used either in the terminal (43) or in the front-end processing of the application server (45 of Fig. 4) and/or authentication sever (46 of Fig. 4) and it will be obvious for those skilled in the art that the said demodulator and converter have to use the decoding technique associated to the encoding technique used by the modulator module (60). In this embodiment, the FSK (frequency-shift keying) technique is preferably used, however other techniques could be used, including ASK (amplitude-shift keying) or PSK (phase-shift keying).

Fig. 7 depicts another embodiment, where the acoustic interface is used to input data to be processed by the processing unit. In the case, the acoustic signal is output by the terminal (43). Depending on the nature of this terminal, the said acoustic signal can be generated either by the terminal (if this terminal is a P.C. or digital telephone) or by the application server peripherals (if the terminal is a simple analog telephone). The acoustic signal is received by means of the microphone

(71), demodulated and converted to a digital signal by the demodulation module (70) and then passed to the processing unit (10) for processing. The demodulation and analog to digital conversion is well known in the art and will not be described here. Again, the demodulator must use the decoding technique corresponding to the encoding technique used by the modulator (either in the terminal or server peripherals). In this embodiment, the FSK (frequency-shift keying) technique is preferably used, however other techniques could be used, including ASK (amplitude-shift keying) or PSK (phase-shift keying).

Still another embodiment of the invention is depicted by Fig. 8, where the acoustic interface is used both for data input and output. This is obviously a combination of embodiments previously described with Fig. 6 and Fig. 7. It should be noted that the encoding and decoding techniques used respectively by the modulator (60) and demodulator (70) need not necessarily to be the same. However, in a preferred embodiment, FSK technique is used for both.

Fig. 9 depicts a preferred embodiment of the configuration shown by Fig. 8, where the speaker is used as a bi-directional acoustic transducer, so that no microphone is needed. This configuration will be preferred in most cases, except when very high sensitivity is required for data input from the acoustic interface.

By way of example, a few applications of the invention will be described below. However, it will be apparent for those skilled in the art that the features of this invention are not limited thereto but may be applied in a wide variety of other applications.

A first application of the invention consists in using the PCD for access control to a restricted area (e.g.: a building, a room, a parking place, etc.). In this case, a microphone is placed at the entrance of the restricted area and anybody willing to access the said area has to use his or her PCD for generation of valid access code. A

verification server located either in the said area or in a remote site connected to the said area is used to verify the code and to permit access when the code is valid. Similarly, the PCD can be used for user authentication before allowing access to a local and/or remote resource, including protected machine and/or vehicle, sensitive database, private network, etc.

Besides the access control, transaction certification is another typical application of the invention. For example, remote payments by phone or P.C. networks (e.g. Internet) can be certified using the data authentication capability of the invention. In this case, the PCD is used to generate a digital signature ensuring the authenticity of the data received by the application server.

Furthermore, the PCD can also be used as a efficient and user-friendly encryption tool. For this application, the preferred embodiment will be equipped with bi-directional acoustic interface (as depicted in Fig. 8 and 9), so that automatic data transfer can easily be achieved between the PCD and a large variety of communication terminals. By way of example, such application may consists in allowing telephone use of a smart card based electronic purse, for remote payment and/or loading of the said electronic purse.

The foregoing description has been limited to what are currently believed to be the preferred embodiments and applications of the present invention. However, those skilled in the art will realize that variations and modifications may be made thereto without departing from the true spirit of the invention and it is intended in the appended claims to cover all such variations and modifications as come within the true spirit and scope of the present invention.

What we claim is:

1. A portable certification device comprising a compact housing provided at least with:

a) first means selected from the group consisting of :

- data storage means for storage of at least one cryptographic key,

- a means for at least reading information from a smart card containing at least one cryptographic key, and

- any combination thereof ;

b) at least one acoustic interface for wireless exchange of information with the device, by means of at least an acoustic signal generated using a modulation technique selected from the group consisting of : frequency-shift keying, phase-shift keying, amplitude-shift keying and any combination thereof;

c) processing means, at least for processing signal between the acoustic interface and said processing means;

d) means for supplying power to the first means, processing means and acoustic interface.

2. The device of claim 1, in which the modulation technique is frequency-shift keying.

3. The device of claim 1, in which at least one acoustic interface is used to input data to be processed by the processing means.

4. The device of claim 1, in which at least one acoustic interface is used to output data processed by the processing means.

5. The device of claim 1, in which at least one acoustic interface is used to input data to be processed by the processing means and to output data processed by the processing means.

6. The device of claim 5, wherein different modulation techniques are used for input and output of data.

7. The device of claim 1, wherein a smart card interface is provided, for smart card data interchange.

8. The device of claim 1, which is further provided with at least one non-acoustic interface for data interchange.

9. The device of claim 1, wherein the processing means comprise an algorithm selected from the group consisting of : algorithm for unique user identification, algorithm for data authentication, algorithm for data encryption, and any combination thereof.

10. The device of claim 1, comprising a means for at least reading information from a smart card, the said smart card comprising an algorithm selected from the group consisting of : algorithm for unique user identification, algorithm for data authentication, algorithm for data encryption, and any combination thereof.

11. The device of claim 1, wherein the processing means comprise a first algorithm selected from the group consisting of : algorithm for unique user identification, algorithm for data authentication, algorithm for data encryption, and any combination thereof, the said device further comprising a means for at least reading information from a smart card, the said smart card comprising a second algorithm selected from the group consisting of : algorithm for unique user identification, algorithm for data authentication, algorithm for data encryption, and any combination thereof ; the said second algorithm being different from the first.

12. The device of claim 1, which comprises data storage means for at least one cryptographic key.

13. The device of claim 1, which comprises a means for at least reading information from a smart card containing at least one cryptographic key.

14. The device of claim 1, which comprises data storage means for at least a first cryptographic key and a means for at least reading information from a smart card containing at least a second cryptographic key, different from the first one.

15. The device of claim 1, which further comprises initialization means.

16. The device of claim 15, wherein the said initialization means are associated to radio signal reception means.

17. The device of claim 1, which further comprises user interface means, allowing control of the device.

18. The device of claim 17, in which the user interface means include at least a keypad.

19. The device of claim 1, which further comprises user interface means, allowing control of the device, said user interface means comprising at least on/off switching means.

20. The device of claim 1, which further comprises user interface means, allowing control of the device, said user interface means comprising at least a user display.

21. The device of claim 1, which comprises at least a microphone as acoustic interface.

22. The device of claim 1, which comprises at least means selected from the group consisting of speaker, buzzer and any combination thereof, as acoustic interface.

23. The device of claim 1, which comprises at least a speaker used as bi-directional acoustic interface.

24. The device of claim 1, in which the processing means process at least a signal by means of an algorithm using at least one cryptographic key.

25. A certification method having the improvement of exchanging data by means of at least an acoustic signal generated using a modulation technique selected from the group consisting of : frequency-shift keying, phase-shift keying, amplitude-shift keying and any combination thereof.

26. The method of claim 25 in which the modulation technique is frequency-shift keying.

27. The method of claim 25 applied for access control.

28. The method of claim 25 applied for user authentication.

29. The method of claim 25 applied for certifying remote transactions.

30. The method of claim 25 applied for data authentication.

31. The method of claim 25 applied for data encryption.

5

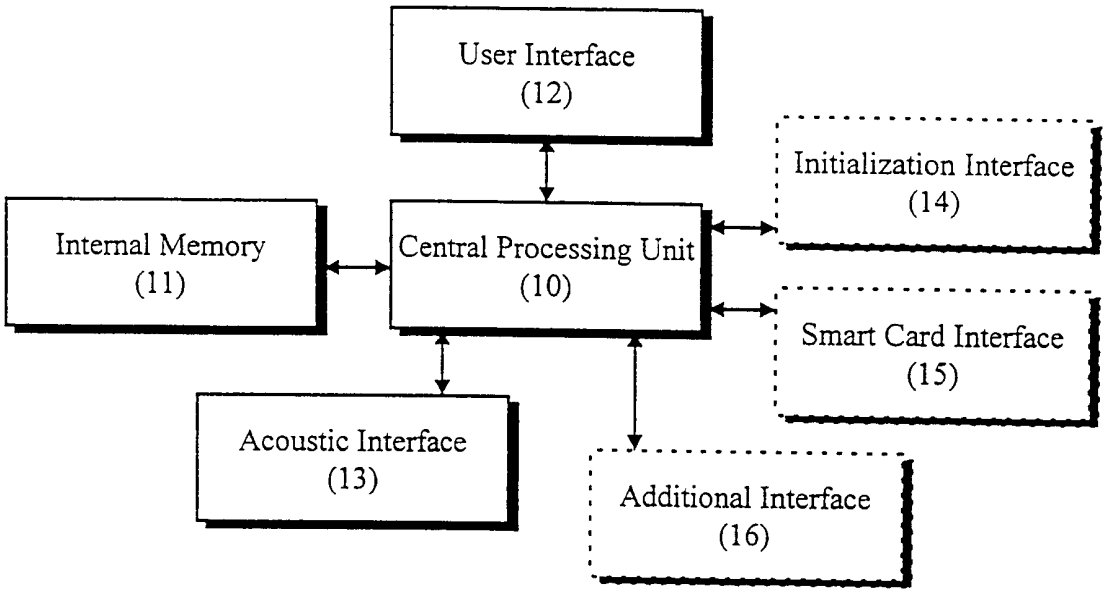

User Interface
(12)
Initialization Interface
(14)
Internal Memory
(11)
Central Processing Unit
(10)
Smart Card Interface
(15)
Acoustic Interface
(13)
Additional Interface
(16)

Figure 1

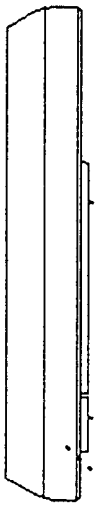


Figure 2B

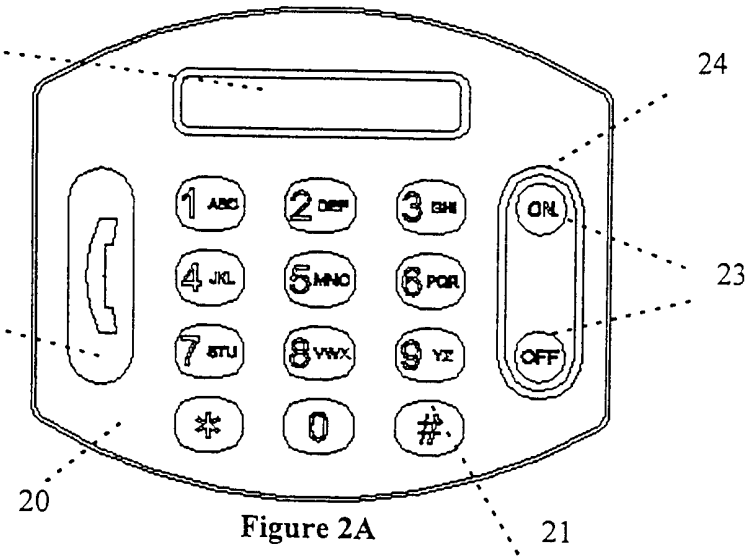


Figure 2A

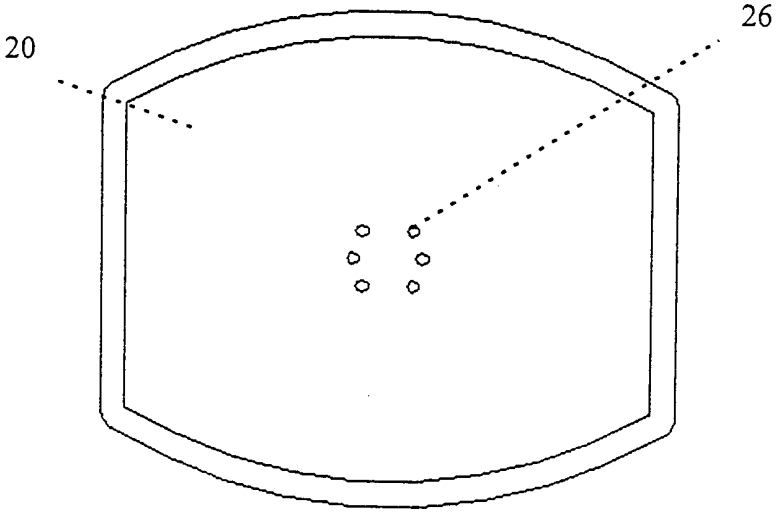


Figure 2C

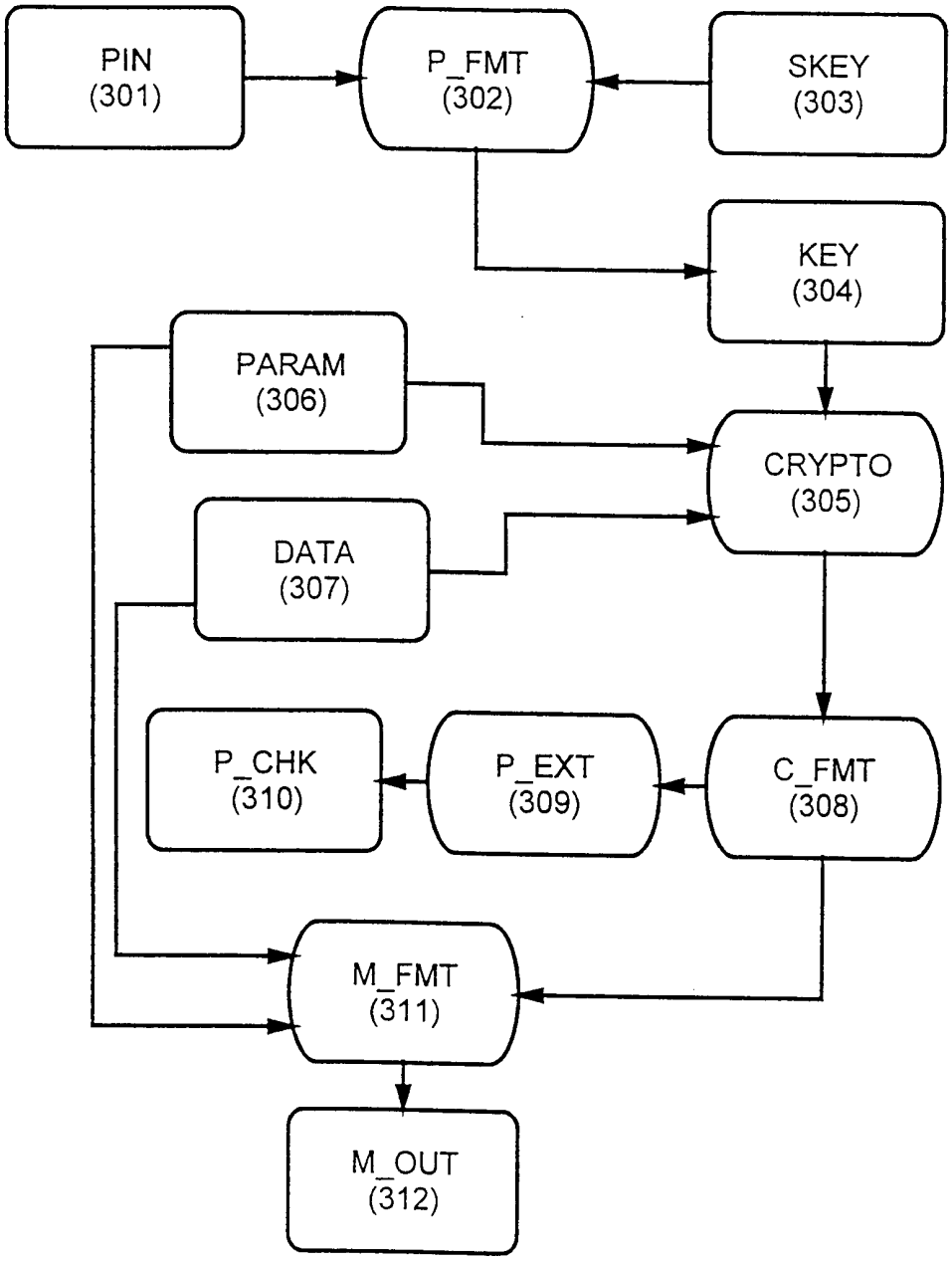

PIN
(301)
P_FMT
(302)
SKEY
(303)
KEY
(304)
PARAM
(306)
CRYPTO
(305)
DATA
(307)
P_CHK
(310)
P_EXT
(309)
C_FMT
(308)
M_FMT
(311)
M_OUT
(312)

Figure 3

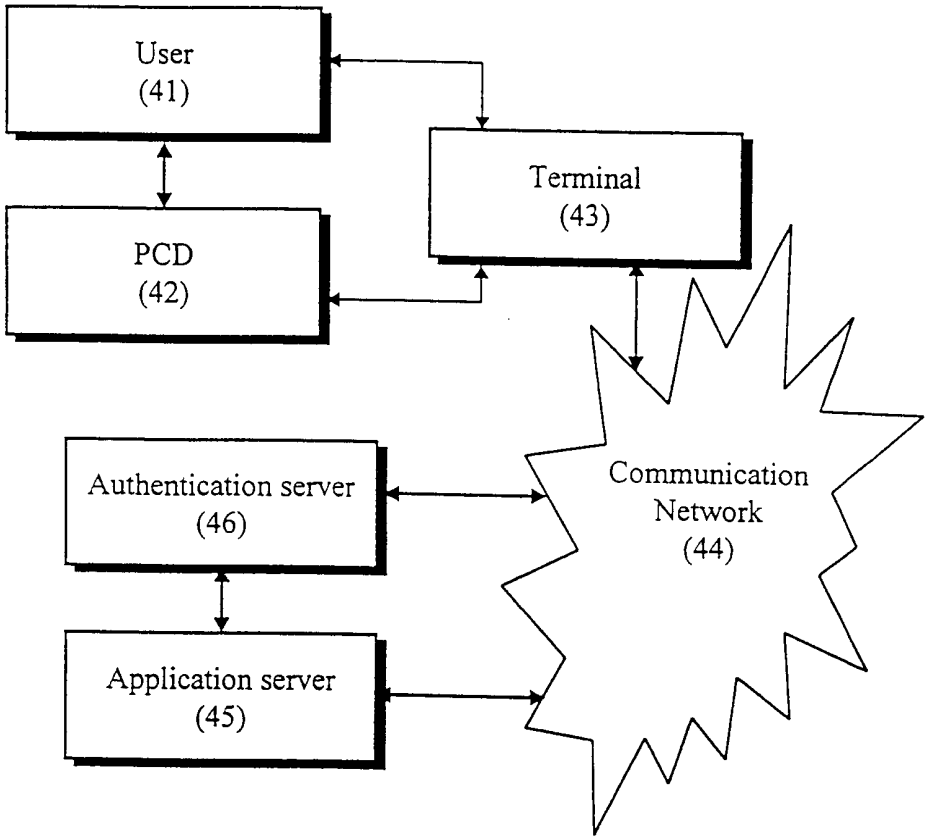


Figure 4

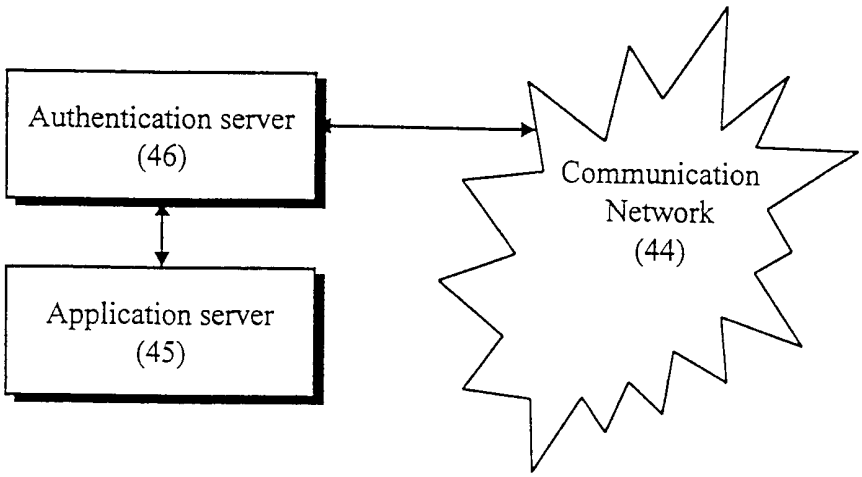


Figure 5

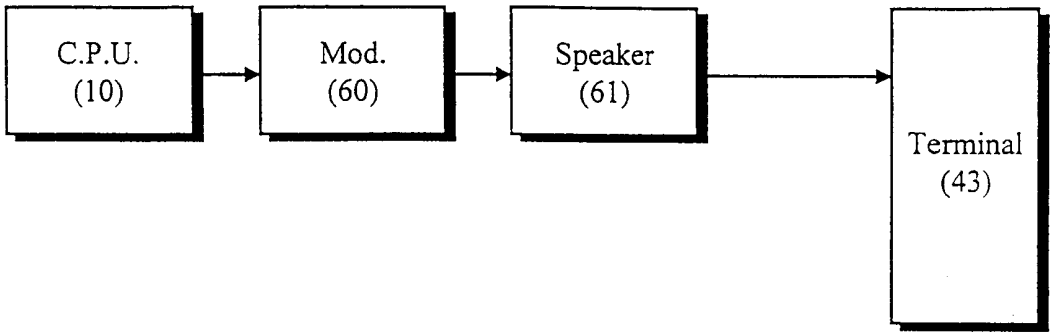


Figure 6

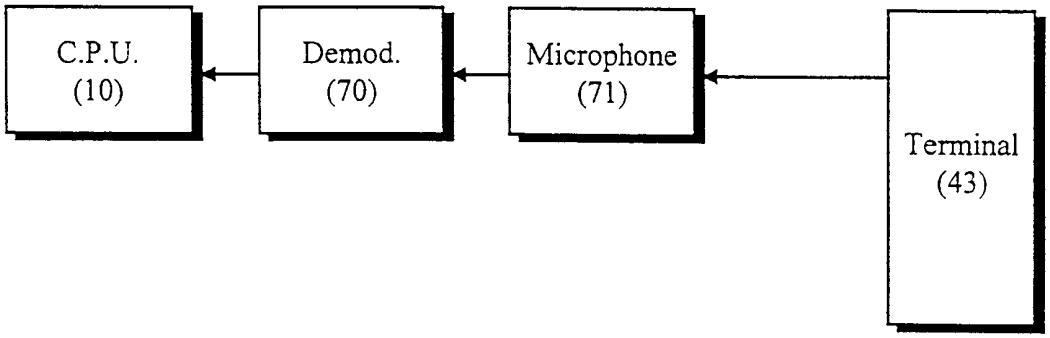


Figure 7

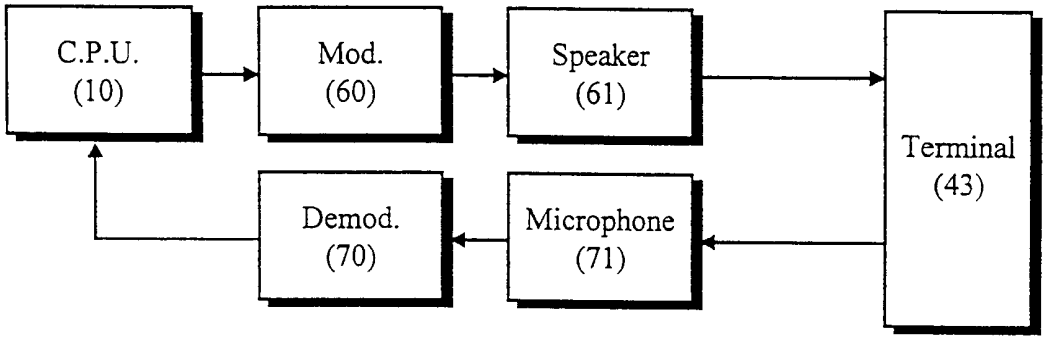


Figure 8

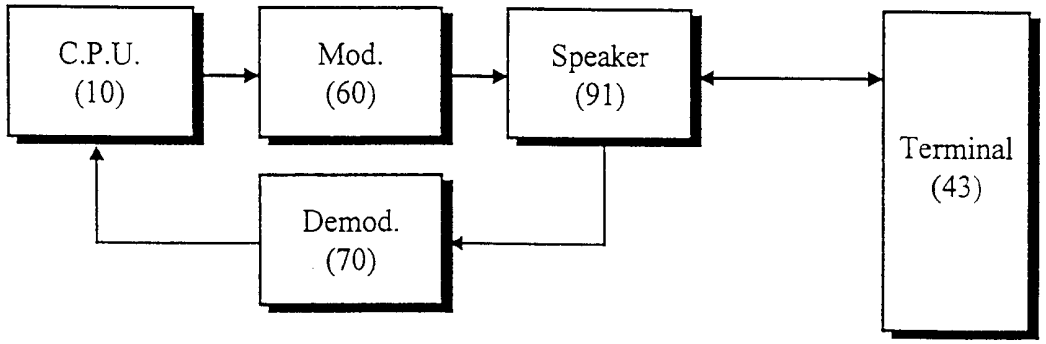


Figure 9

INTERNATIONAL SEARCH REPORT

Inte .ional Application No
PCT/BE 00/00092

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

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 7 G07F

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 43 25 459 A (C2S CRYPTOGRAFISCHE SICHERHEITSSYSTEME) 9 February 1995 (1995-02-09)	1,4,7-9, 12, 17-20, 22,24-30
A	the whole document	2,5,10, 13,31

X	EP 0 374 012 A (ETAT FRANCAIS) 20 June 1990 (1990-06-20)	1,3-5,9, 17, 21-24,28
A	the whole document	12,15,27

A	US 5 740 232 A (J-C. PAILLES) 14 April 1998 (1998-04-14)	1,2,4, 7-13, 17-20, 22,24-30
	the whole document	

	-/--	

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

[X] Patent family members are listed in 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
8 December 2000	15/12/2000

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte .ional Application No
PCT/BE 00/00092

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 95 10823 A (BRITISH TELECOMMUNICATIONS) 20 April 1995 (1995-04-20) abstract; claims; figures page 16, line 3 - line 9	1-5,8,9, 17-22, 25-28
A	US 5 878 142 A (A.A. CAPUTO) 2 March 1999 (1999-03-02)	
A	EP 0 565 279 A (AMERICAN TELEPHONE AND TELEGRAPH) 13 October 1993 (1993-10-13)	
A	US 4 601 011 A (A. GRYNBERG) 15 July 1986 (1986-07-15)	
A	US 5 818 930 A (E.R. MARK) 6 October 1998 (1998-10-06)	
A	WO 98 25371 A (Y. YANG) 11 June 1998 (1998-06-11)	

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte .ional Application No
PCT/BE 00/00092

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4325459 A	09-02-1995	NONE	
EP 0374012 A	20-06-1990	FR 2640835 A	22-06-1990
US 5740232 A	14-04-1998	FR 2719730 A	10-11-1995
		EP 0710386 A	08-05-1996
		WO 9530975 A	16-11-1995
		JP 8512419 T	24-12-1996
WO 9510823 A	20-04-1995	CA 2171345 A	20-04-1995
		DE 69409972 D	04-06-1998
		DE 69409972 T	10-09-1998
		EP 0740819 A	06-11-1996
		ES 2117303 T	01-08-1998
		HU 74344 A	30-12-1996
		JP 9503877 T	15-04-1997
		SG 49729 A	15-06-1998
		US 5606614 A	25-02-1997
US 5878142 A	02-03-1999	US 5546463 A	13-08-1996
		US 5778071 A	07-07-1998
EP 0565279 A	13-10-1993	AT 153159 T	15-05-1997
		AU 3533093 A	07-10-1993
		CA 2087886 A,C	07-10-1993
		DE 69310604 D	19-06-1997
		DE 69310604 T	04-09-1997
		ES 2101227 T	01-07-1997
		HK 1002716 A	11-09-1998
		JP 6046162 A	18-02-1994
		US 5406619 A	11-04-1995
US 4601011 A	15-07-1986	DE 3248400 A	28-07-1983
		GB 2114791 A	24-08-1983
US 5818930 A	06-10-1998	US 5583933 A	10-12-1996
		AU 3239795 A	04-03-1996
		CA 2196784 A	15-02-1996
		EP 0774189 A	21-05-1997
		JP 10508161 T	04-08-1998
		WO 9604741 A	15-02-1996
		US 5907597 A	25-05-1999
		US 5825871 A	20-10-1998
		US 5745555 A	28-04-1998
		US 5732133 A	24-03-1998
		US 6014441 A	11-01-2000
		US 5949874 A	07-09-1999
WO 9825371 A	11-06-1998	US 5917913 A	29-06-1999
		AU 5383198 A	29-06-1998