



(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
H04L 9/14 (2006.01)

(21) International Application Number:
PCT/US2009/033413

(22) International Filing Date:
6 February 2009 (06.02.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/028,220 8 February 2008 (08.02.2008) US

(71) Applicant (for all designated States except US): **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, M3-2B, San Francisco, California 94128 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HAMMAD, Ayman** [US/US]; 6048 Corte Montanas, Pleasanton, California 94566 (US). **FAITH, Patrick** [US/US]; 2810 Jones Gate Court, Pleasanton, California 94566 (US).

(74) Agents: **JEWIK, Patrick R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111-3834 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) Title: KEY DELIVERY SYSTEM AND METHOD

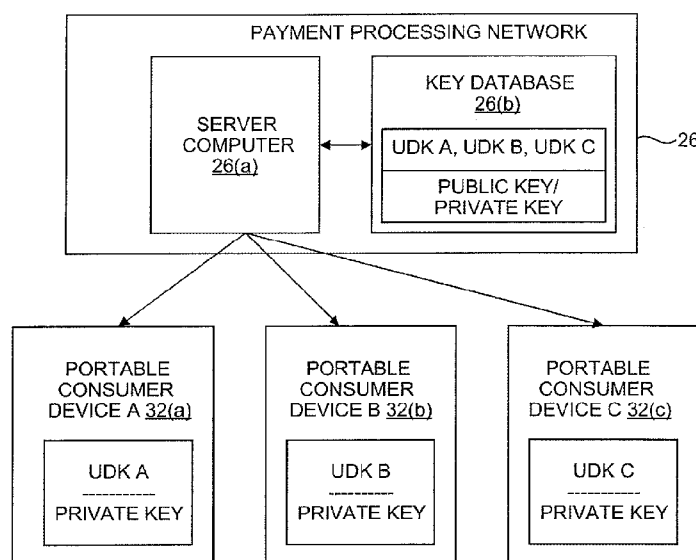


FIG. 2

(57) Abstract: A method for delivering a key is disclosed. The method includes encrypting a first key using a second uniquely derived key to form an encrypted first key, and providing the encrypted first key to a transaction device. The transaction device contains the second uniquely derived key.

KEY DELIVERY SYSTEM AND METHOD

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] NOT APPLICABLE

BACKGROUND

[0002] It would be desirable to have a process whereby a portable consumer device could "sign" transaction data associated with a transaction (e.g., a purchase transaction) that is being conducted by the portable consumer device, so that the recipient of the transaction data can verify that the portable consumer device being used is in fact authentic. One way to provide for this is to provide the portable consumer device with a private key in a public/private key pair. Transaction data can be signed using the private key in the portable consumer device. The transaction data can then be sent to a recipient who can verify the digital signature associated with the signed data using the public key of the public/private key pair.

[0003] One problem to be solved is how to deliver the private key to the portable consumer device. An issuer may issue many portable consumer devices to thousands of consumers. It is difficult to securely deliver private keys to the various portable consumer devices.

[0004] Embodiments of the invention address the above problems, and other problems, individually and collectively.

SUMMARY

[0005] Embodiments of the invention are directed to systems, methods, portable consumer devices that can securely deliver encryption keys to transaction devices such as portable consumer devices. In embodiments of the invention, a uniquely derived key (UDK) can be used to encrypt and deliver a key to a portable consumer device operated by a consumer. The UDK is derived from information that is specifically associated with the consumer. Alternatively or additionally, the information may be specifically associated with a portable consumer device that is

associated with the consumer. For example, such information may include an account number associated with the consumer, an expiration date associated with the portable consumer device, etc. Once the UDK is derived, it can be used to encrypt a key such as a private key of a public/private key pair. The encrypted private key can be securely provided to (e.g., sent to) the portable consumer device. After the encrypted key is received at the portable consumer device, the portable consumer device can use a derived or previously stored UDK to decrypt the encrypted key. Once the key is decrypted, it is secure in the portable consumer device and can be used. For instance, if the key is a private key in a public/private key pair, then the private key can thereafter be used to digitally sign data to authenticate the portable consumer device in a transaction such as a purchase transaction.

[0006] One embodiment of the invention is directed to a method comprising encrypting a first key using a second uniquely derived key to form an encrypted first key. The method also includes providing the encrypted first key to a transaction device such as a portable consumer device, where the transaction device contains the second uniquely derived key.

[0007] Another embodiment of the invention is directed to a computer readable medium comprising code for encrypting a first key using a second uniquely derived key to form an encrypted first key and code for providing the encrypted first key to a transaction device. The portable consumer device contains the second uniquely derived key.

[0008] Another embodiment of the invention is directed to a method comprising receiving an encrypted first key. The first key was previously encrypted using a uniquely derived key. After the encrypted first key is received, the first key is decrypted using the uniquely derived key.

[0009] Another embodiment of the invention is directed to a computer readable medium comprising code for receiving an encrypted first key. The first key was previously encrypted using a uniquely derived key. The computer readable medium further comprises code for decrypting the encrypted first key using the uniquely derived key.

[0010] Another embodiment of the invention is directed to a portable consumer device comprising a computer readable medium. The computer readable medium comprises code for a uniquely derived key and code for a public key or a private key of a public/private key pair.

[0011] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 shows a flowchart illustrating a method according to an embodiment of the invention.

[0013] FIG. 2 shows a block diagram showing the distribution of keys in various portable consumer devices.

[0014] FIG. 3 shows a block diagram illustrating a method for forming a uniquely derived key.

[0015] FIG. 4 shows a block diagram of a system according to an embodiment of the invention.

[0016] FIG. 5 shows a flowchart illustrating a method according to an embodiment of the invention.

[0017] FIG. 6(a) shows a block diagram illustrating components in a phone.

[0018] FIG. 6(b) shows components that may be in a typical payment card.

[0019] FIG. 7 shows a block diagram of components in a computer apparatus.

DETAILED DESCRIPTION

[0020] One embodiment of the invention is directed to a method comprising encrypting a first key using a second uniquely derived key to form an encrypted first key. The method also includes providing the encrypted first key to a transaction device such as a portable consumer device, where the transaction device contains the second uniquely derived key. The transaction device may store the second uniquely derived key in a memory.

[0021] In the specific embodiments below, a "transaction device" in the form of a portable consumer device is described in detail. It is understood that a transaction device could also include an access device. In embodiments of the invention, an encrypted key may be delivered to any suitable transaction device at one end of a transaction so that the transaction device may sign transaction data that may be received by a second transaction device at another end of the transaction, whereby the second transaction device (e.g., a server computer in a payment processing network) verifies the signed data using a corresponding key. Thus, although the delivery of an encrypted key to a portable consumer device is described in detail below, the same principles may be applied to delivery of an encrypted key to another type of transaction device such as an access device.

[0022] I. Key delivery

[0023] Embodiments of the invention are directed to systems, methods, portable consumer devices that can securely deliver encryption keys, etc. In embodiments of the invention, a uniquely derived key (UDK) can be used to encrypt and deliver a first key such as a private key in a public/private key pair, to a portable consumer device operated by a consumer.

[0024] The UDK is derived from information that is specifically associated with the consumer. Alternatively or additionally, the information may be specifically associated with a portable consumer device that is associated with the consumer. For example, such information may include an account number associated with the consumer, an expiration date associated with the portable consumer device, a consumer's social security number, a consumer's telephone number, etc. In other embodiments, the UDK may be derived from other types of data. For example, if the UDK is intended for delivery to an access device such as a POS terminal, then the information that is used to generate the UDK may include information such as a terminal ID, location, date of manufacture, etc.

[0025] Once the UDK is derived, it can be used to encrypt a key, such as a private key of a public/private key pair, so that it can be securely delivered to a portable consumer device. After the encrypted private key is received at the portable consumer device, the portable consumer device can use a derived or previously stored UDK to decrypt the encrypted private key. Once the private key is decrypted,

it is secure in the portable consumer device and can be used. The private key can be used to digitally sign data to authenticate the portable consumer device in a transaction such as a purchase transaction.

[0026] In the preferred embodiments that are described herein, the key that is encrypted and delivered to the portable consumer device is a private key in a public/private key pair. It is understood that embodiments of the invention are not limited to this. For example, the encrypted key that is delivered to the portable consumer device could be a symmetric private key, or could even be a public key in a public/private key pair.

[0027] It is also noted that although the use of a "public" key is described in detail, it is understood that in embodiments of the invention, a public key may or may not be available to the general public. It can be "public" in the sense that someone other than holder of the private key knows about the public key. For instance, in some cases, the public key may be known to a merchant, issuer, payment processing organization, and acquirer, but may not be known or available to the general public.

[0028] Embodiments of the invention have a number of advantages. For example, it is difficult for an unauthorized person to decrypt any private key that has been encrypted with a uniquely derived key. To decrypt the encrypted key, the unauthorized person would have to know the uniquely derived key that was used to encrypt the private key. Since the uniquely derived key is uniquely derived, it is difficult for the unauthorized person to determine. Also, even if the unauthorized person was able to determine the uniquely derived key, knowledge of a particular uniquely derived key would only be useful for a single account. Knowledge of one uniquely derived key will not necessarily apply to other uniquely derived keys, since each key is uniquely derived using unique data.

[0029] FIG. 1 shows a flowchart illustrating an embodiment of the invention. As shown in FIG. 1, a uniquely derived key can be derived (step 102). Once the uniquely derived key is derived, it can be used to encrypt a key such as a private key of a public/private key pair (step 104). Once the key is encrypted, it can be delivered to a portable consumer device (step 106). Once the portable consumer device receives the encrypted key, the portable consumer device can decrypt the encrypted

key using the uniquely derived key that is stored or derived within the portable consumer device (step 108). Once the encrypted key is decrypted, it may be used by the portable consumer device (step 110). For example, the portable consumer device may use the key to sign data to provide an electronic signature. Data may be subsequently received, and the electronic signature may be verified to ensure that the data was generated using an authentic portable consumer device.

[0030] The steps shown in FIG. 1 may be further described with reference to FIGS. 2 and 3. FIG. 2 shows a diagram of some components of a key distribution system. FIG. 3 shows a block diagram illustrating how a uniquely derived key can be formed in one embodiment of the invention.

[0031] FIG. 2 shows a block diagram of a key distribution system. The system includes a payment processing network 26 and a number of portable consumer devices 32(a), 32(b), 32(c). The payment processing network 26 may comprise a server computer 26(a) and a key database 26(b) operatively coupled to the server computer 26(a). In this example, the payment processing network 26 may be operated by a payment processing organization such as Visa™. However, in other embodiments, the server computer 26(a) and the key database 26(b) may be operated by another entity such as an issuer or a third party payment processor.

[0032] Referring to both FIGS. 1 and 2, first, a uniquely derived key may be derived for each portable consumer device 32(a), 32(b), 32(c) (step 102). If the uniquely derived key is not generated on an as needed basis, it may be derived beforehand and may be stored in the key database 26(b). As shown in FIG. 2, a uniquely derived key A may be created for portable consumer device A 32(a), a uniquely derived key B may be created for portable consumer device B 32(b), and a uniquely derived key C may be created for portable consumer device C 32(c). Since each uniquely derived key (e.g., UDKs A, B, and C) is generated using data personal to the consumers operating the specific portable consumer devices (e.g., portable consumer devices A, B, and C), the uniquely derived keys (UDKs A, B, and C) could be generated by the portable consumer devices A, B, and C (32(a)-32(c)) if they have the same UDK generation algorithm that the payment processing network 26 possesses. Alternatively, they can be previously generated (e.g., by the server

computer 26(a) or some other computer apparatus) and stored in the portable consumer devices A, B, and C 32(a), 32(b), 32(c).

[0033] An exemplary process for forming a uniquely derived key may be described with reference to FIG. 3. An account number 201, an account sequence number 202, an inverse of the account number 203, and an inverse of the account sequence number 204 are concatenated together to create a concatenated value 210. If necessary, the concatenated value 210 may be padded with zeroes, or some other value 211, to create a string of a predetermined fixed length. In a preferred embodiment, the concatenated value 210 may be 128 bits in length, although the concatenated value is not limited to being this length. The concatenated value 210 is then encrypted 220 using the master derivation key 221 as the encryption key for each encryption stage. The encryption utilized may include any suitable type of encryption methodology. For example, this encryption step may utilize DES, Triple-DES, or AES encryption algorithms. The value resulting from the encryption step 220 is a unique derived key or UDK 230. If desired, the UDK 230 may be further processed to form another UDK. For example, the UDK 230 may be segmented into different parts, and a particular part of the UDK may form a UDK that can be used to encrypt a key. This might be done to make the UDK of suitable length for the selected key encryption process.

[0034] Second, once a uniquely derived key is obtained, the private key of the public/private key PAIR is encrypted using the uniquely derived key (step 104). For example, the payment processing network 26 may use the server computer 26(a) to encrypt a private key of the public/private key pair. The encryption process may use an algorithm such as a DES or Triple DES algorithm.

[0035] Third, the encrypted key is provided to the portable consumer device (step 106). In some embodiments, the server computer 26(a) may provide the encrypted private key to the portable consumer device A 32(a) via some intermediate entity such as a third party processor. If the portable consumer device A 32(a) is in the form of a phone or a portable computer, the encrypted key may be provided (e.g., downloaded) from the server computer 26(a) to the phone or portable computer via an appropriate communications network (e.g., a wireless network, the Internet, etc.).

[0036] Fourth, after the encrypted private key is received by the portable consumer device A 32(a), it is decrypted at the portable consumer device 32(a) (step 108). The portable consumer device A 32(a) may decrypt the encrypted private key using the uniquely derived key A that is in portable consumer device A 32(a). Once the encrypted private key is decrypted, it may be stored within a secure hardware element inside of the portable consumer device A 32(a). It can thereafter be used to digitally sign transaction data associated with a transaction conducted using the portable consumer device.

[0037] II. Purchase Transactions

[0038] A. Exemplary Transaction Systems

[0039] A method of using the delivered public/private key system can be described with reference to FIGS. 4-5.

[0040] FIG. 4 shows a block diagram of a purchase transaction system. Embodiments of the invention are not limited to the described embodiments. For example, although separate functional blocks are shown for an issuer, payment processing system, and acquirer, in FIG. 4, some entities perform all of these functions and may be included in embodiments of invention.

[0041] FIG. 4 shows a system that can be used in an embodiment of the invention. The system includes a merchant 22 and an acquirer 24 associated with the merchant 22. In a typical payment transaction, a consumer 30 may purchase goods or services at the merchant 22 using a portable consumer device A 32(a). The acquirer 24 can communicate with an issuer 28 via a payment processing network 26.

[0042] The payment processing network 26 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network operated by the payment processing organization 20 may include VisaNet™. Payment processing systems such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP

system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0043] The payment processing network 26 may include a server computer 26(a). A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may also have a processor and a computer readable medium, which comprises code or instructions that the processor can execute. For example, it may comprise code for encrypting a first key using a second uniquely derived key to form an encrypted first key, and code for providing the encrypted first key to a transaction device, where the portable consumer device contains the second uniquely derived key. The payment processing network 26 may use any suitable wired or wireless network, including the Internet.

[0044] The merchant 24 may also have, or may receive communications from, an access device 34 that can interact with the portable consumer device 28(a). The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0045] If the access device 34 is a point of sale terminal, any suitable point of sale terminal may be used including card readers. The card readers may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device 28(a). It may comprise a computer readable medium comprising code for receiving an encrypted first key, where the first key was previously encrypted using a uniquely derived key, and code for decrypting the encrypted first key using the uniquely derived key.

[0046] B. Exemplary Purchase Methods

[0047] Referring to FIGS. 4 and 5, in a typical purchase transaction, the consumer 30 purchases a good or service at the merchant 22 using the portable consumer device A 32(a) (step 112). The consumer's portable consumer device A 32(a) can interact with an access device 34 such as a POS (point of sale) terminal at the merchant 22. Using the portable consumer device A 28(a) and the private key present therein, the portable consumer device A may sign transaction data and this data may be incorporated into the authorization request message that is to be forward to the acquirer 24 by the access device 34 (step 114). The transaction data may include consumer specific information such as an account number, expiration date, birthday, social security number, etc. Transaction data may also include purchase information such as SKU information, purchase price information, etc.

[0048] Before or after the access device 34 receives the signed transaction data, the signed data may be preprocessed on in any suitable manner. For example, the signed data may undergo truncation or decimalization processing before it is incorporated into an authorization request message, and is forwarded by the access device 34 to the payment processing network 26 via the acquirer 24.

[0049] After receiving the authorization request message, the authorization request message is then sent to the payment processing network 26.

[0050] The payment processing network 26 then receives the signed data (step 116). It then uses the public key of the public/private key pair is used to verify that the signed data are authentic (step 118). The public key, which may be stored in the key database 26(b) can be used to decrypt the signed data and the decrypted information can be verified (e.g., a decrypted account number can be matched with other data in the authorization request message or other data that are stored in a database in the payment processing network 26).

[0051] Since the public key is public and can be known by someone other than the consumer 30 or the consumer's portable consumer device 32(a), the public key can also be sent to the issuer 28, acquirer 24, or even the merchant 22. Using the public key, any of these entities may verify the signed data provided portable consumer device 32(a). Thus, embodiments of the invention are not limited to verification of signed data by a payment processing network 26.

[0052] After the signed data are verified, the payment processing network 26 then forwards the authorization request message to the issuer 18 of the portable consumer device 32(a).

[0053] After the issuer 18 receives the authorization request message, the issuer 18 sends an authorization response message back to the payment processing system 20 to indicate whether or not the current transaction is authorized (or not authorized). If there are insufficient funds or credit in the consumer's account, the transaction may be declined. If there are sufficient funds or credit in the consumer's account, the transaction may be authorized. The payment processing system 20 then forwards the authorization response message back to the acquirer 22. The acquirer 22 then sends the response message back to the merchant 24.

[0054] After the merchant 22 receives the authorization response message, the access device 34 at the merchant 22 may then provide the authorization response message for the consumer 30. The response message may be displayed by the POS terminal, or may be printed out on a receipt.

[0055] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing system 20. A clearing process is a process of exchanging financial details between an acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position. Clearing and settlement can occur simultaneously.

[0056] III. Portable consumer devices and computer apparatuses

[0057] FIGS. 6-7 shows block diagrams of portable computer devices and subsystems that may be present in computer apparatuses in systems according to embodiments of the invention.

[0058] The portable consumer device that is used in embodiments of the invention may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal

digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0059] An exemplary portable consumer device 32' in the form of a phone may comprise a computer readable medium and a body as shown in FIG. 6(a). (FIG. 6(a) shows a number of components, and the portable consumer devices according to embodiments of the invention may comprise any suitable combination or subset of such components.) The computer readable medium 32(b) may be present within the body 32(h), or may be detachable from it. The body 32(h) may be in the form a plastic substrate, housing, or other structure. The computer readable medium 32(b) may be a memory that stores data and may be in any suitable form including a magnetic stripe, a memory chip, uniquely derived keys (such as those described above), encryption algorithms, private keys, etc. It may comprise code for receiving an encrypted first key, where the first key was previously encrypted using a uniquely derived key, and code for decrypting the encrypted first key using the uniquely derived key. The memory also preferably stores information such as financial information, transit information (e.g., as in a subway or train pass), access information (e.g., as in access badges), etc. Financial information may include information such as bank account information, bank identification number (BIN), credit or debit card number information, account balance information, expiration date, consumer information such as name, date of birth, etc.

[0060] Information in the memory may also be in the form of data tracks that are traditionally associated with credits cards. Such tracks include Track 1 and Track 2. Track 1 ("International Air Transport Association") stores more information than Track 2, and contains the cardholder's name as well as account number and other discretionary data. This track is sometimes used by the airlines when securing reservations with a credit card. Track 2 ("American Banking Association") is currently most commonly used. This is the track that is read by ATMs and credit card checkers. The ABA (American Banking Association) designed the specifications of this track and all world banks must abide by it. It contains the cardholder's account, encrypted PIN, plus other discretionary data.

[0061] The portable consumer device 32 may further include a contactless element 32(g), which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Contactless element 32(g) is associated with (e.g., embedded within) portable consumer device 32 and data or control instructions transmitted via a cellular network may be applied to contactless element 32(g) by means of a contactless element interface (not shown). The contactless element interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry (and hence the cellular network) and an optional contactless element 32(g).

[0062] Contactless element 32(g) is capable of transferring and receiving data using a near field communications ("NFC") capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as RFID, BluetoothTM, infra-red, or other data transfer capability that can be used to exchange data between the portable consumer device 32 and an interrogation device. Thus, the portable consumer device 32 is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0063] The portable consumer device 32 may also include a processor 32(c) (e.g., a microprocessor) for processing the functions of the portable consumer device 32 and a display 32(d) to allow a consumer to see phone numbers and other information and messages. The portable consumer device 32 may further include input elements 32(e) to allow a consumer to input information into the device, a speaker 32(f) to allow the consumer to hear voice communication, music, etc., and a microphone 32(i) to allow the consumer to transmit her voice through the portable consumer device 32. The portable consumer device 32 may also include an antenna 32(a) for wireless data transfer (e.g., data transmission).

[0064] If the portable consumer device is in the form of a debit, credit, or smartcard, the portable consumer device may also optionally have features such as magnetic strips. Such devices can operate in either a contact or contactless mode.

[0065] An example of a portable consumer device 32" in the form of a card is shown in FIG. 6(b). FIG. 6(b) shows a plastic substrate 32(m). A contactless element 32(o) for interfacing with an access device 34 may be present on or embedded within the plastic substrate 32(m). Consumer information 32(p) such as an account number, expiration date, and consumer name may be printed or embossed on the card. Also, a magnetic stripe 32(n) may also be on the plastic substrate 32(m).

[0066] As shown in FIG. 6(b), the portable consumer device 32" may include both a magnetic stripe 32(n) and a contactless element 32(o). In other embodiments, both the magnetic stripe 32(n) and the contactless element 32(o) may be in the portable consumer device 32". In other embodiments, either the magnetic stripe 32(n) or the contactless element 32(o) may be present in the portable consumer device 32".

[0067] The various participants and elements in FIG. 2 and 4 may operate or use one or more computer apparatuses to facilitate the functions described herein. Any of the elements in FIG. 2 and 4 may use any suitable number of subsystems to facilitate the functions described herein. Examples of such subsystems or components are shown in FIG. 7. The subsystems shown in FIG. 7 are interconnected via a system bus 775. Additional subsystems such as a printer 774, keyboard 778, fixed disk 779 (or other memory comprising computer readable media), monitor 776, which is coupled to display adapter 782, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 771, can be connected to the computer system by any number of means known in the art, such as serial port 777. For example, serial port 777 or external interface 781 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor 773 to communicate with each subsystem and to control the execution of instructions from system memory 772 or the fixed disk 779, as well as the exchange of information between subsystems. The system memory 772 and/or the fixed disk 779 may embody a computer readable medium.

[0068] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon

review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0069] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0070] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0071] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 encrypting a first key using a second uniquely derived key to form an
3 encrypted first key; and
4 providing the encrypted first key to a transaction device, wherein the
5 transaction device includes the second uniquely derived key.
- 1 2. The method of claim 1 wherein the first key is a private key of a
2 public/private key pair, and wherein the transaction device is a portable consumer
3 device.
- 1 3. The method of claim 1 wherein providing the encrypted first key
2 to the transaction device comprises downloading the encrypted first key to the
3 transaction device.
- 1 4. The method of claim 1 wherein the encrypted first key is
2 subsequently decrypted in the transaction device using the second uniquely derived
3 key.
- 1 5. The method of claim 1 wherein the transaction device is a
2 portable consumer device that is in the form of a payment card.
- 1 6. A computer readable medium comprising:
2 code for encrypting a first key using a second uniquely derived key to
3 form an encrypted first key; and
4 code for providing the encrypted first key to a transaction device,
5 wherein the transaction device contains the second uniquely derived key.
- 1 7. The computer readable medium of claim 6 wherein the first key
2 is a private key of a public/private key pair.
- 1 8. The computer readable medium of claim 6 wherein providing the
2 encrypted first key to the transaction device comprises downloading the encrypted
3 first key to the transaction device.
- 1 9. A server computer comprising a processor, and the computer
2 readable medium of claim 6 operatively coupled to the processor.

1 10. A server computer comprising a processor, and the computer
2 readable medium of claim 7 operatively coupled to the processor.

1 11. A method comprising:
2 receiving an encrypted first key, wherein the first key was previously
3 encrypted using a uniquely derived key; and
4 decrypting the encrypted first key using the uniquely derived key.

1 12. The method of claim 11 wherein the encrypted first key is
2 decrypted in a portable consumer device.

1 13. The method of claim 11 wherein the first key is a public key in a
2 public/private key pair.

1 14. The method of claim 11 further comprising:
2 signing data using the first key; and
3 providing the signed data to an entity.

1 15. The method of claim 11 wherein receiving and decrypting are
2 performed by a portable consumer device.

1 16. A computer readable medium comprising:
2 code for receiving an encrypted first key, wherein the first key was
3 previously encrypted using a uniquely derived key; and
4 code for decrypting the encrypted first key using the uniquely derived
5 key.

1 17. The computer readable medium of claim 16 wherein the first key
2 is a public key in a public/private key pair.

1 18. The computer readable medium of claim 16 further comprising:
2 code for signing data using the first key; and
3 code for providing the signed data to an entity.

1 19. A portable consumer device comprising the computer readable
2 medium of claim 16.

- 1 20. A portable consumer device comprising a computer readable
2 medium, wherein the computer readable medium comprises code for a uniquely
3 derived key and code for a public key or a private key of a public/private key pair.

1 / 7

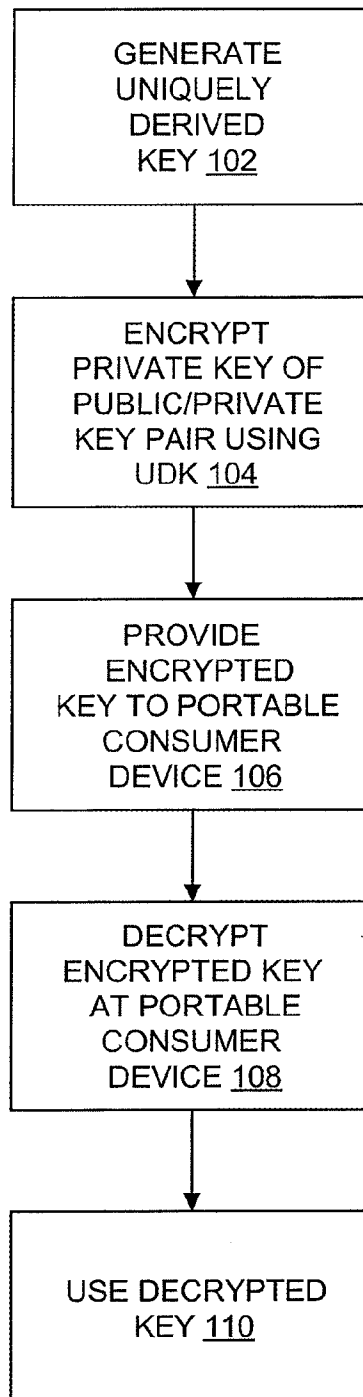


FIG. 1

2 / 7

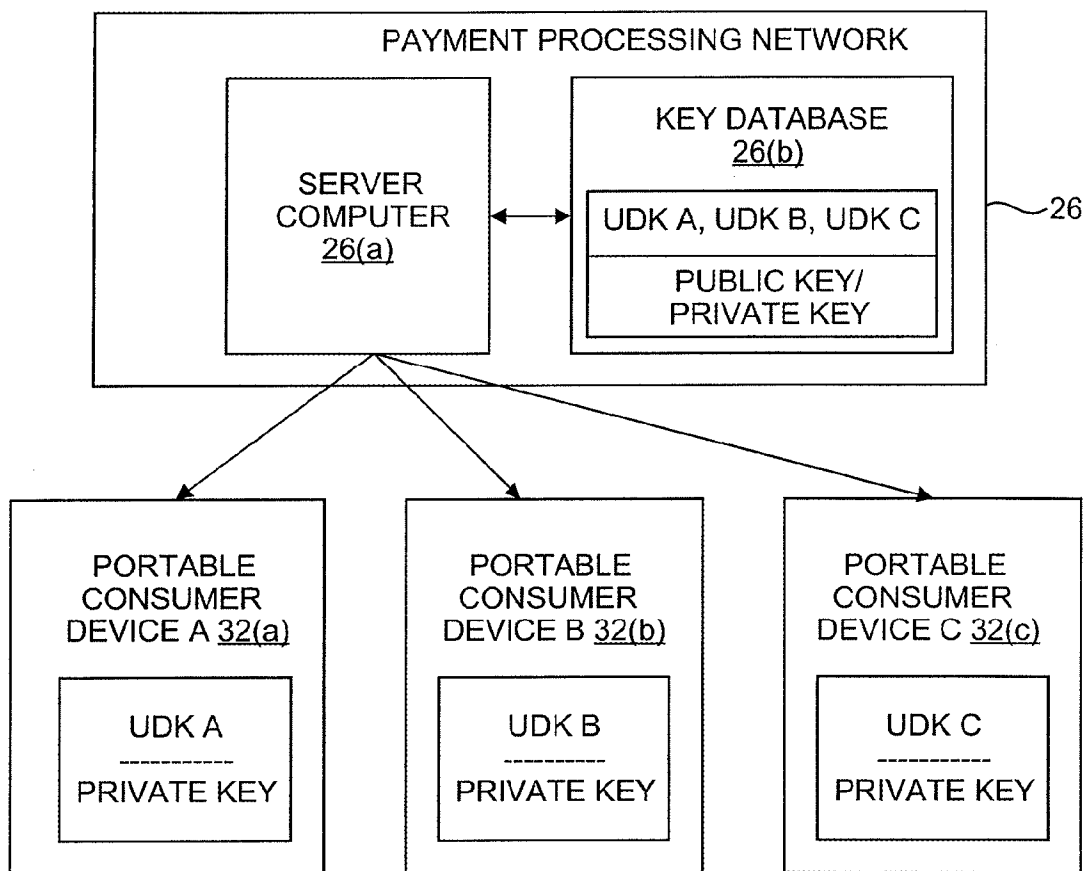


FIG. 2

3 / 7

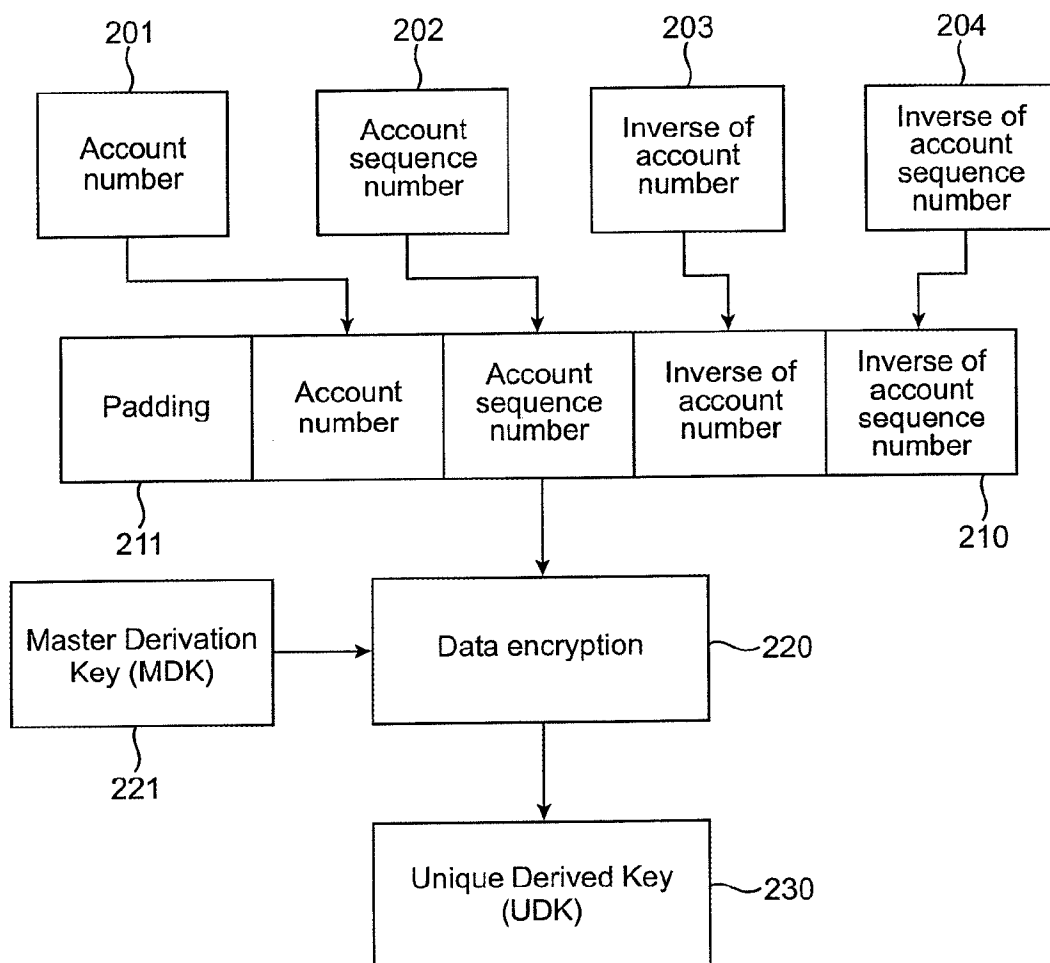


FIG. 3

4 / 7

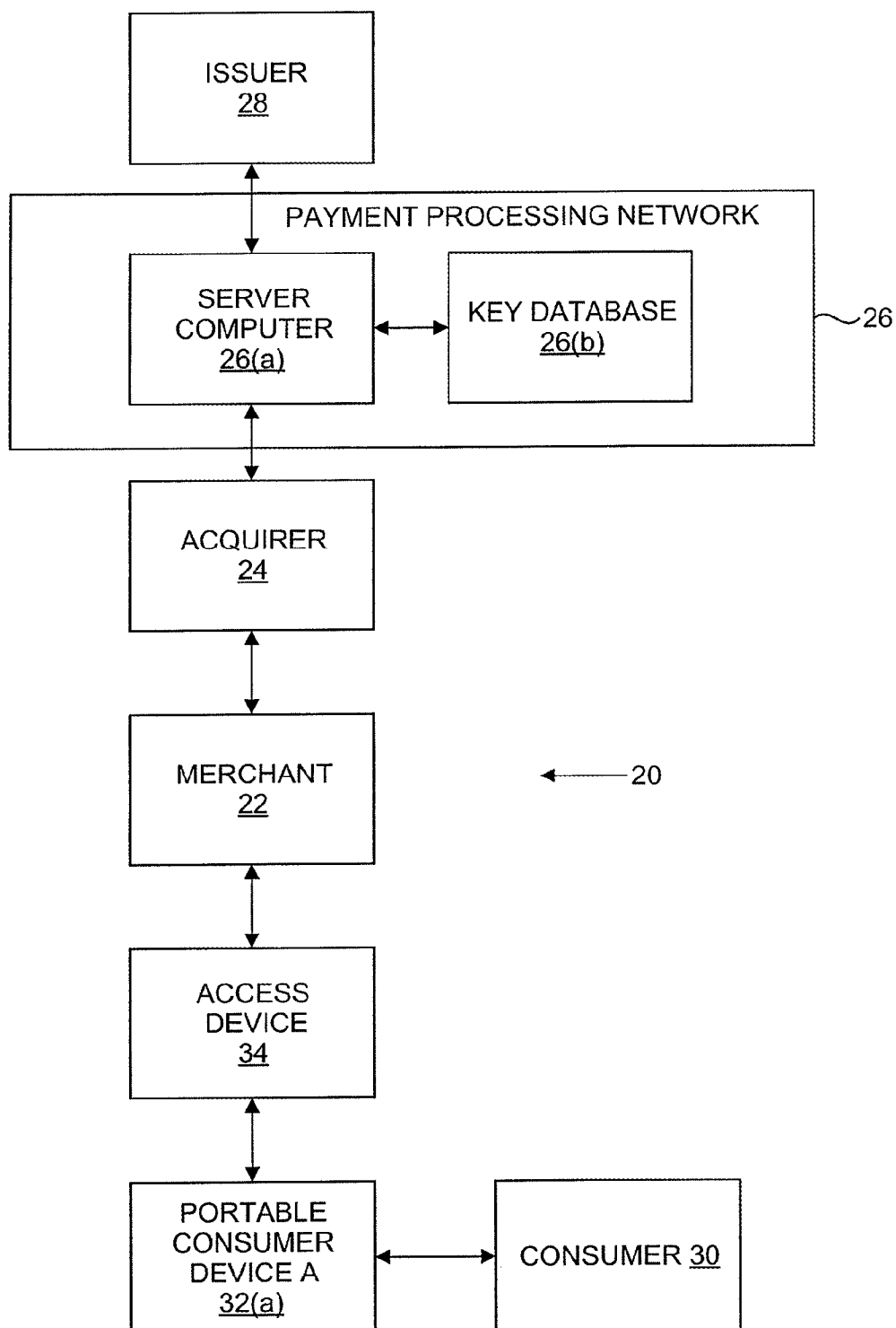


FIG. 4

5 / 7

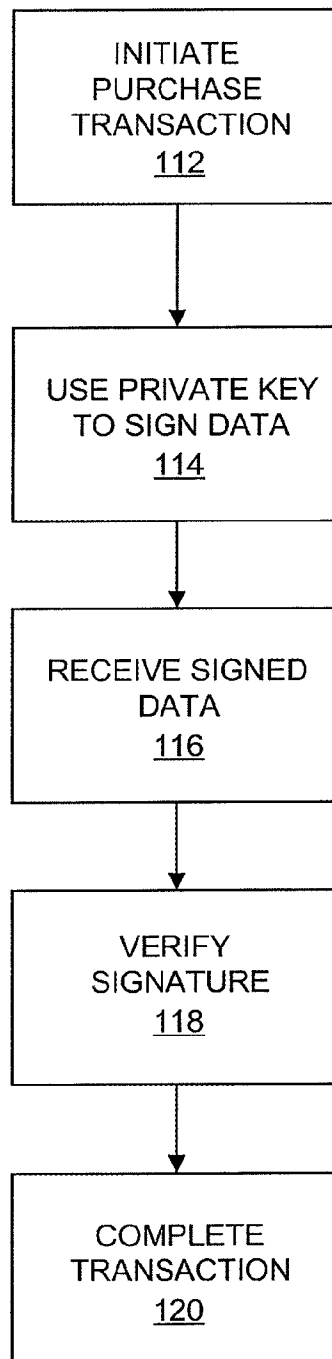


FIG. 5

6 / 7

32'

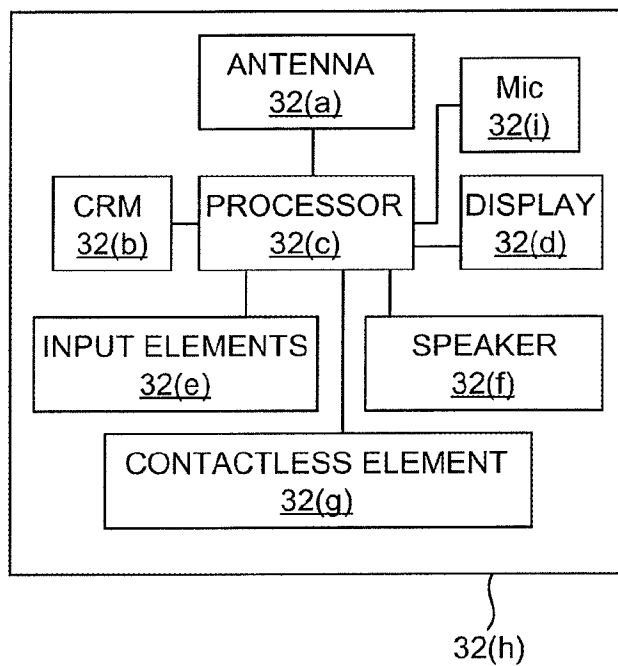


FIG. 6(a)

32''

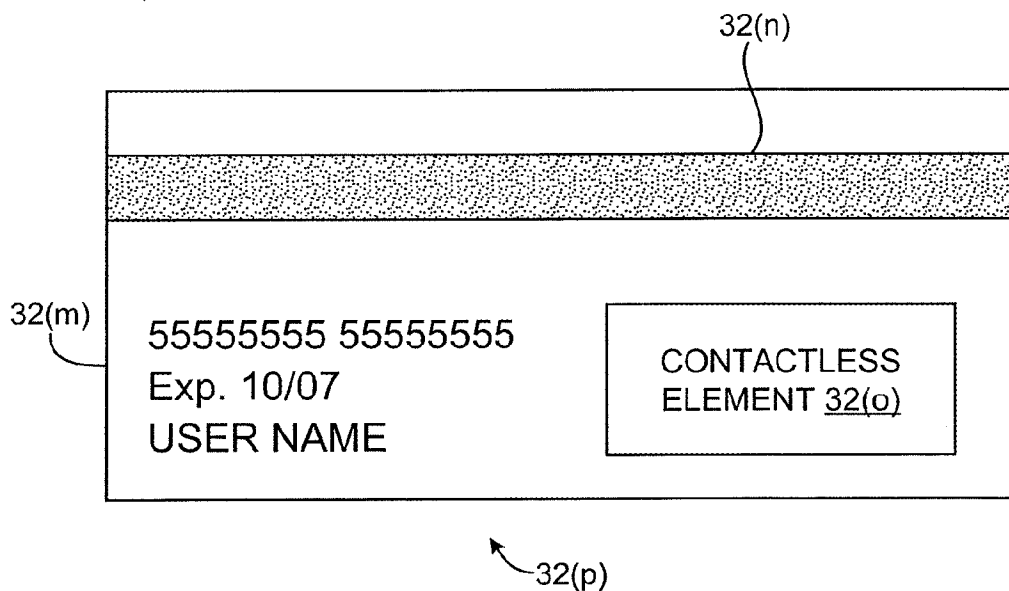


FIG. 6(b)

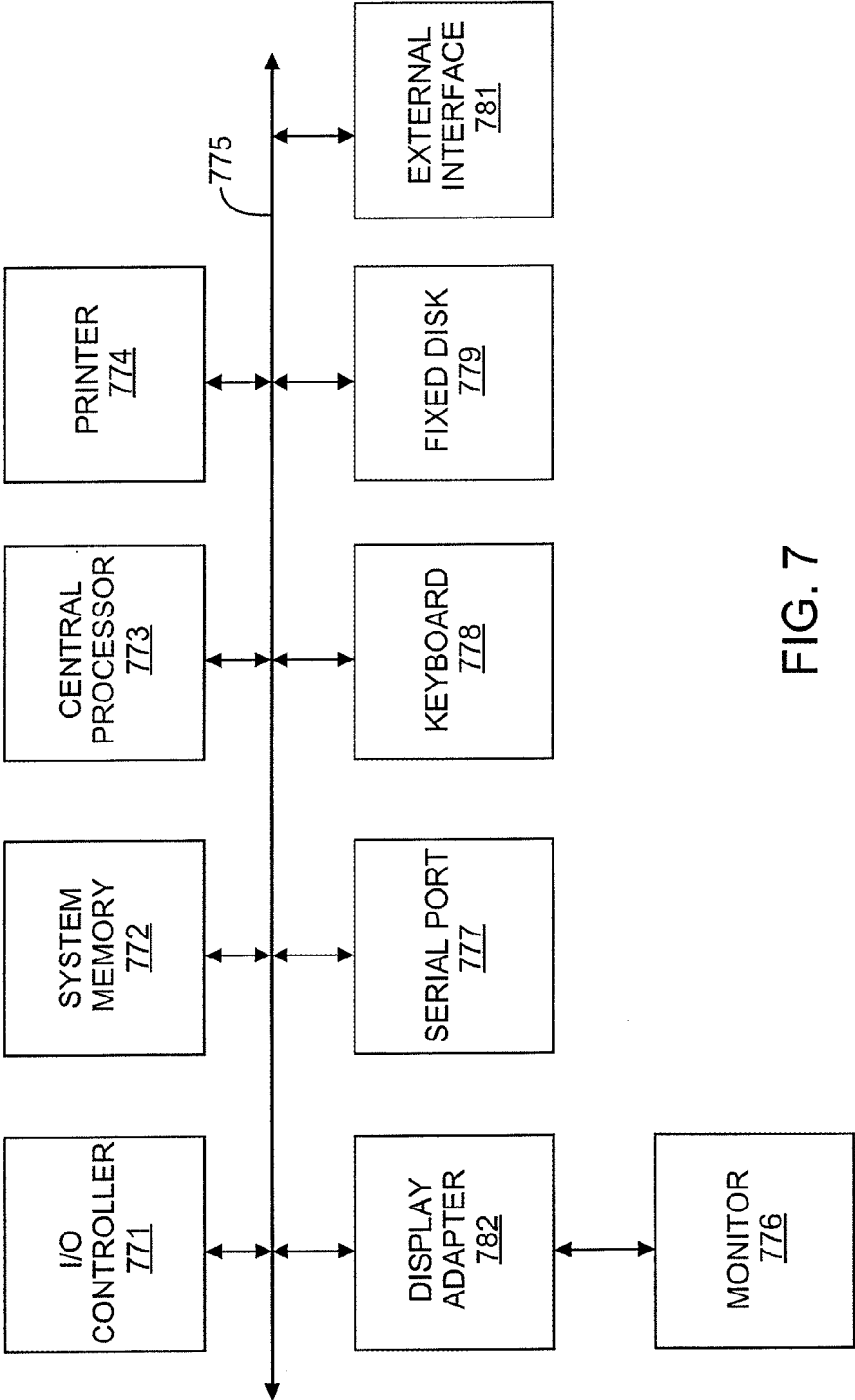


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/033413**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/08(2006.01)i, H04L 9/14(2006.01)i, H04L 9/30(2006.01)i**

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: H04L, G06K, G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
KOREAN UTILITY MODELS AND APPLICATIONS FOR UTILITY MODELS SINCE 1975
JAPANESE UTILITY MODELS AND APPLICATIONS FOR UTILITY MODELS SINCE 1975Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKIPASS (KIPO internal) & keywords : UDK, encryption**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2008-0029593 A1 (AYMAN HAMMAD et al.) 07 February 2008 See abstract; claims 1, 10, 14, 15 and figures 1, 2, 6, 7.	20 1-19
A	US 6925182 B1 (MICHAEL A. EPSTEIN) 02 August 2005 See abstract; claim 1 and figures 1, 2.	1-20
A	US 2004-0101141 A1 (JUKKA ALVE) 27 May 2004 See abstract; claims 1-3, 10, 11 and figures 1-3.	1-20
A	WO 01-61906 A2 (CITIBANK, N.A.) 23 August 2001 See abstract; claim 1 and figure 1.	1-20

☐ 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 application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of 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

30 JUNE 2009 (30.06.2009)

Date of mailing of the international search report

02 JULY 2009 (02.07.2009)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-
gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

YANG, Jeong Rok

Telephone No. 82-42-481-5709



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/033413

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0029593 A1	07.02.2008	AU 2004-267784 A1	03.03.2005
		CA 2536208 A1	03.03.2005
		EP 1656600 A2	17.05.2006
		JP 2007-513529 A	24.05.2007
		KR 10-2006-0117902 A	17.11.2006
		US 2005-0043997 A1	24.02.2005
		WO 2005-020012 A2	03.03.2005
=====			
US 6925182 B1	02.08.2005	CA 2281719 A1	01.07.1999
		EP 0965200 A1	22.12.1999
		JP 2001-512654 A	21.08.2001
		TW 429722 B	11.04.2001
		WO 99-33219 A1	01.07.1999
=====			
US 2004-0101141 A1	27.05.2004	AU 2003-280082 A1	18.06.2004
		CN 1726668 A	25.01.2006
		EP 1579620 A1	28.09.2005
		EP 1579620 A4	04.01.2006
		KR 10-2005-0086885 A	30.08.2005
		WO 2004-049620 A1	10.06.2004
=====			
WO 01-61906 A2	23.08.2001	AU 6096401 A	27.08.2001
		US 7076061 B1	11.07.2006
		WO 01-61906 A3	31.01.2002