PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00, H04Q 1/00 — A1

(11) International Publication Number: WO 99/56429

(43) International Publication Date: 4 November 1999 (04.11.99)

(21) International Application Number: PCT/US99/08990

(22) International Filing Date: 26 April 1999 (26.04.99)

(30) Priority Data:
09/066,643 24 April 1998 (24.04.98) US
09/298,326 23 April 1999 (23.04.99) US

(71) Applicant: IDENTIX INCORPORATED [US/US]; 510 North Pastoria Avenue, Sunnyvale, CA 94086 (US).

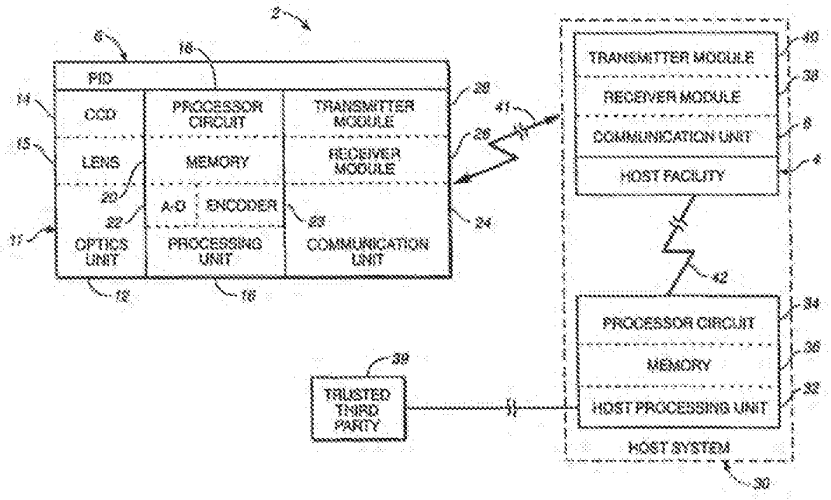
(72) Inventors: SCOTT, John, D.; 9 Pine Valley Road, Galston, NSW 2159 (AU). CURTIS, Terence, P.; 10 Selina Avenue, Katoomba, NSW 2250 (AU).

(74) Agent: GARCIA, Edouard, A.; Fish & Richardson P.C., Suite 100, 2200 Sand Hill Road, Menlo Park, CA 94025 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: PERSONAL IDENTIFICATION SYSTEM AND METHOD



(57) Abstract

A portable, hand-held personal identification device (6) and method for providing secure access to a host facility (4) includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative of the sensed biometric trait. A processing unit responsive to the biometric signal is adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is unique to the enrolled person, and to provide a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person. The verification signal (41) includes information indicative of the enrolled person or the device. A communication unit, including a transmitting circuit (28), is adapted to transmit the verification signal to a host system (30).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

PERSONAL IDENTIFICATION SYSTEM AND METHOD

Background of the Invention

The invention relates to a personal identification system and method for allowing access to secure facilities.

Some security systems, such as home security systems and door locks, require a user to enter a fixed code into a device at a host facility before allowing a person access to the facility. Other systems, such as automated teller machines (ATM), require a person to submit an authorized card and also to enter a fixed code that is associated with the person's bank accounts. Automobile alarms, locks, and disabling devices, and garage door openers can be operated by pressing a button on a small remote device to transmit a coded signal to a receiving unit on the automobile or garage.

Each of these security systems can be operated by any person who is in possession of the fixed code, the card or the transmitting device, as the case may be. Therefore, each of these systems is inherently insecure. Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility. The biometric trait is a unique identifier of a person, and can be, for example, a person's fingerprint, voice pattern, iris pattern, or the like. The requesting person also enters other identifying information about himself. The measured biometric trait is compared with stored biometric data associated with the identified person and, if there is a match, the requesting person is allowed entry or access to the host facility.

In presently available biometric systems, each authorized person registers with the host facility by providing a sample of their biometric trait, for example, by having his fingerprint optically scanned into a host system data base. Each host facility must have a biometric sensor, access to the database of registered persons' biometric trait registration data, and a processing system capable of quickly searching the database and conducting the comparison to verify a person's identity. However, if the set of authorized persons is large, such a system would require a huge database to store the fingerprint images of all the authorized persons, and the

identification process would become slower as the set of authorized persons increases.

Summary of the Invention

According to one aspect of the invention, a portable personal identification device for providing secure access to a host facility includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative thereof. A processing circuit responsive to the biometric signal is adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person. The processor provides a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person. The verification signal is indicative of the enrolled person or the device. A communication unit, including a transmitter circuit, is adapted to transmit the verification signal to a remote host system.

In another aspect, the invention features a personal identification system, comprising: a biometric sensor configured to extract a representation of a biometric trait of a user; a processor configured to verify the user's identity based upon a comparison of a representation of a biometric trait extracted from a user with a stored representation of the biometric trait; and a transmitter configured to transmit a verification signal indicative of a successful verification of the user's identity.

Embodiments may include one or more of the following features. The processor may be configured to process signals received from a global positioning system (GPS) receiver. The processor may be configured to derive trip information (e.g., the location of the GPS receiver) from the signals received from the GPS receiver. The processor may be programmable to prompt the user for additional verification information when the GPS receiver is positioned at a particular location.

The system may include a user input configured to enable a user to enter trip information, and wherein the processor is configured to process information

received from the user. The transmitter may be further configured to transmit signals representative of stored trip information.

The biometric sensor, the processor, and the transmitter may be housed within a portable, hand-held housing. The system may include an input device mounted inside a vehicle and coupled to the vehicle's power system, and wherein the input device is adapted to receive the verification signal from the transmitter and to enable the user to turn on the vehicle only upon receipt of the verification signal. The housing may have the form of a pocket-sized security badge. The housing may be configured to receive a graphical representation of the user.

The system may include an automatic door locking device coupled to a vehicle door (or trunk) and adapted to unlock the door (or trunk) upon receipt of the verification signal. The system also may include a receiver. The processor may be operable to switch the system from a low power operation to a normal power operation when the receiver receives a power-up signal from a host system. The system also may include a memory configured to store the representation of the biometric trait. The memory may be housed within a portable housing separable from the biometric sensor, processor and transmitter.

The communication unit preferably is adapted for remote communication with the host system via a wireless communication medium. The device can further include a display and a keypad.

The biometric sensor system can include a fingerprint sensor, a voice sensor, or any other type of biometric sensor. The fingerprint sensor can include a platen adapted for placing a finger thereon. The fingerprint sensor can further include an optical image sensor, which may include a complementary metal oxide semiconductor (CMOS) optical sensor, a charge coupled device (CCD) optical sensor, or any other optical sensor having sufficient resolution to provide a signal indicative of a fingerprint image. In the embodiments with an optical sensor, the platen would include an optical platen, and the biometric sensor may also include a lens focusing light from the platen onto the optical sensor. The fingerprint sensor can alternatively include a direct contact sensor device, such as a capacitive sensor chip or thermal sensor chip. In these embodiments, the platen would be the surface of the sensor chip.

The processing unit can include a processor circuit, a memory and an encoder, wherein the memory stores the biometric data, and wherein the verification signal includes an encrypted signal encrypted by the encoder. In one embodiment, the encoder includes an encoding circuit, and the verification signal further includes an ID code indicative of the enrolled person or the device.

In another embodiment, the encoder comprises an encryption algorithm programmed into the processor. The encryption algorithm employs a private key indicative of the enrolled person or the device. In this embodiment, the communication unit can further include a receiver circuit. The memory can further store an ID code indicative of the enrolled person or the device. The processor unit can be further adapted to first cause the transmitter circuit to transmit an ID code signal indicative of the ID code to the host system. The receiver circuit can be adapted to receive a host response signal transmitted by the host system in response to the ID code signal. The processor unit employs the encryption algorithm and the private key to encrypt the host response signal to create the verification signal, and causes the transmitter circuit to transmit the verification signal to the host system only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person.

In either of these embodiments, the memory can be located in a removable plug-in module, and the personal identification device further includes a socket adapted to receive the module.

According to another aspect of the invention, a portable, hand-held personal identification device for providing secure access to a host facility includes a housing. A fingerprint sensor system in the housing is capable of sensing a fingerprint of a user and providing a fingerprint signal indicative thereof. The fingerprint sensor system includes a platen on a surface of the housing adapted to receive a finger. A communication unit in the housing is adapted for wireless communication with a separate host system. The communication unit includes a transmitting circuit and a receiving circuit. A slot in the housing receives a removable smart card that includes a memory. The device can be combined with the smart card. The memory in the smart card stores a fingerprint template representative of the fingerprint of an enrolled person, and an ID code and a

personal encryption key being associated with the device. A processing circuit in the device is adapted to cause the ID code signal from memory to be transmitted by the transmitting circuit. The processing circuit is further adapted to cause a host response signal received by the receiving circuit signal from the host system in response to the ID code signal to be encrypted according an encryption algorithm employing the personal encryption key and to cause the encrypted host response signal to be transmitted by the transmitting circuit only if the fingerprint signal corresponds sufficiently to the fingerprint template to verify that the user is the registered person.

According to yet another aspect of the invention, a method of providing secure access to a host facility includes the step of registering one or more persons with the host facility, including storing a unique ID code and a public encryption key for each registered person. The method also includes receiving a first transmission comprising a first user signal at the host facility, generating and then transmitting a random number signal from the host facility only if the first user signal represents one of the stored ID codes, receiving a second transmission comprising a second user signal at the host facility, decrypting the second user signal with the public encryption key associated with the registered person who is also associated with the stored ID code represented by the first user signal, and providing access to the host facility only if the decrypted second user signal represents the random number.

According to still another aspect of the invention, a method of providing access to a secure host facility only to registered persons includes registering one or more registered persons with the host system. Registering each registered person includes storing an ID code associated only with a portable hand-held device under the control of that registered person. The method also includes transmitting an ID code signal from a portable hand-held device to a host facility of the host system. The ID code signal represents an ID code associated with the transmitting device. Other steps include generating, at the host facility, a random number signal representing a random number in response to the ID code signal only if the ID code signal is representative of the ID code of the device controlled by one of the registered persons, and retrieving, with the host system, a public key associated

with the one of the registered persons only if the ID code signal is representative of the ID code of the one the devices controlled by the one of the registered persons. Retrieving the public key can include retrieving the public key from a trusted third party. Further steps include transmitting the random number signal from the host facility to the transmitting device, and receiving the random number signal with the transmitting device. The method also includes generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of the transmitting device, and comparing, with the transmitting device, the user fingerprint signal to a fingerprint template stored in the transmitting device, wherein the fingerprint template represents a fingerprint image of a person who is enrolled with the transmitting device. Other steps include encrypting the random number signal with the transmitting device, the random number signal being encrypted according to an encryption algorithm employing a private key associated only with the transmitting device, transmitting the encrypted random number signal from the transmitting device to the host facility only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person, decrypting the encrypted random number signal with the host system, including employing the retrieved public key, and providing the user access to the host facility only if the decrypted encrypted random number signal represents the random number.

Transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each can include transmitting via a wireless transmission. Transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each can further include transmitting via at least one of a modem, a cable access TV line, and a computer communication medium.

In yet another aspect of the invention, a method of providing a secure function at a host facility only to a registered person includes registering a person with the host facility by storing an ID code associated only with a portable registered device controlled by the registered person, learning a synchronization counter of the registered device, storing an encryption key associated with the

registered device and associating the encryption key of the registered device with the stored ID code. The method also includes generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of a portable user device, comparing, with the user device, the user fingerprint signal to a fingerprint template stored in the user device, the fingerprint template representing a fingerprint image of an enrolled person who is enrolled with the user device, and generating an access signal with the user device only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person, the access signal including an ID code associated only with the user device, button press information representing a requested function, and encrypted data encrypted with an encryption key associated with the user device, the encrypted data including a synchronization counter associated with the user device. The method then includes transmitting the access signal from the user device to the host facility, determining, with the host facility, if the ID code in the access signal matches the stored ID code, retrieving the encryption key of the registered device if the match is successful, employing the encryption key of the registered device to decrypt the encrypted data and determine the synchronization counter of the user device, comparing the synchronization counter of the user device with the synchronization counter of the registered device, and providing the requested function represented by the button press data only if the synchronization counter of the user device matches the synchronization counter of the registered device.

In another aspect, the invention provides a method of accessing a secure host facility, including sensing a biometric trait of a user that is unique to a user with a biometric sensor system of a portable device, and providing a biometric signal indicative of the biometric trait; comparing, with the portable device, the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person; providing a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person; and transmitting the verification signal and an ID code signal to a remote host system, wherein the

ID code signal is indicative of an ID code associated only with the portable device, and wherein the host system provides access to the secure facility in response to the verification signal only if host facility determines that personal device associated with the ID code belongs to a registered person.

The system can be employed to provide secure access to a variety of different types of host facilities. The system can be used to replace security systems employing key card entry, fixed code entry, or a combination of key card and fixed code entry, which are currently employed, for example, with ATM's, gate and garage door openers, burglar alarm systems, point of sale (POS) devices, hotel room locks, and the like. The system can also be configured for use with automotive remote key entry (RKE) systems, automotive alarm systems, and automotive immobilizers.

The personal identification device and system of the invention has several advantages. The system is very private. Persons' biometric data, such as a fingerprint, are not stored in a central database, as with prior art systems using fingerprint identification for security. An electronic template of a user's fingerprint is stored only with their own personal identification device, and is used only for verifying the user's fingerprint. In the embodiment with two-way communication, the host facilities store only an ID code and a public key for each registered person. The ID code may be the serial number of the device, and the public key can be retained by a trusted third party. The private key used by the device is never disclosed.

The personal identification device is compact, being about the same size as an electronic pager. With advances in technology, it could be made even smaller. The personal identification device can be configured such that all the information that is associated with the user, i.e., the ID code, the personal encryption key, and the fingerprint template, is stored in a smart card, which can be transferred between identical devices having the image capture electronics, processing circuit, communication module and power supply. This enables the user to switch devices when one is worn out or broken without having to re-register.

The host system can be installed at host facilities with a minimal expenditure compared with current systems employing fingerprint identification for

security. The biometric sensor is installed in each personal identification device, rather than with the host facility. This configuration also makes retrofitting existing security systems for use with the personal identification device a relatively simple procedure. The point of contact is with the personal identification device, which makes the present system more feasible for use at exposed, public locations, such as with automated teller machines, parked automobiles, and gate entries, where the weather and vandalism can be problems. This also makes the system of the invention more sanitary than other systems that require a person to operate a public terminal, keypad, or fingerprint scanner.

Because each user carries his own fingerprint template in the personal identification device, users can "roam" to many different applications and host facilities without the need to enroll the template at each site. They only need to register prior to use. This can be done over the phone or over computer communication lines, such as the Internet, if only medium level security is required.

The user has total control over the procedure for accessing a host facility. The ID cannot be read unless the user presses the fingerprint reader. The random number transmission and the encrypted random number transmission cannot be "scanned" as the random numbers are different each time access to a host facility is requested. The personal identification device can be used in conjunction with conventional telephone lines or computer network communication lines without any risk of theft.

Personal identification devices could be sold via any retail outlet, for example, as a shrink wrap product. As the units are manufactured with unique ID codes and private keys there is no need to control the sale in any way.

Unlike prior art biometric identification systems, the user is already enrolled by the first use of the personal identification device. This completely eliminates the delays and problems associated with enrolling large numbers of users and storing each user's biometric data.

Other features and advantages will become apparent from the following description, including the drawings and the claims.

Brief Description of the Drawings

FIG. 1 is a block diagram of a security system according to the invention.

FIG. 2 is a block diagram of another embodiment of a security system according to the invention.

FIG. 3. is a perspective view of a personal identification device according to another feature of the invention.

FIGS. 4A, 4B, 4C, and 4D are respective front, side, top and bottom views of an embodiment of a personal identification device.

FIGS. 5A and 5B are respective front and side views of another embodiment of a personal identification device.

FIG. 6 is a front view of a third embodiment of a personal identification device.

FIG. 7 is a flow diagram illustrating an embodiment of a method of accessing a host facility with a personal identification device.

FIG. 8 is a flow diagram illustrating another embodiment of a method of accessing a host facility with a personal identification device.

FIG. 9 is a schematic diagram of an embodiment of the processor unit.

FIGS. 10A and 10B are a perspective and block diagrams, respectively, of a personal identification system.

FIG. 11 is a perspective view of a personal identification system clipped to a user's pocket.

Detailed Description

Referring to FIG. 1, a security system 2 provides access to one or more secure host facilities 4 only to registered persons. A host facility 4 may be a bank, a store, a military base, a computer system, an automobile, a home security system, a gate, or any other facility where it is desired to restrict access to selected individuals. Each registered person uses a battery powered, portable personal identification device (PID) 6, which communicates with a communication unit 8 located at each host facility 4. PID 6 is small enough to carry on ones person, being similar in size to a hand-held pager. An example of a PID 6 is shown being held in the palm of a man's hand 10 in FIG. 3.

PID 6 includes a biometric sensor. In the described embodiment, a biometric sensor 11 includes an optics unit 12 having a CMOS optical sensor imaging device 14, and an exposed optical platen 15. Imaging device 14 can also be a CCD imaging device. A lens (not shown) may also be used to focus an image from a surface of platen 15 onto imaging device 14. PID also includes a processing unit 16. Processing unit 16 includes a processor circuit 18, an external memory 20 and may include an analog-to-digital converter circuit (A/D) 22. Some CMOS optical sensors provide a digital output signal, which eliminated the need for A/D 22. PID 6 further includes a communication unit 24, which has a transmitter module 26 and a receiver module 28.

Memory 20 stores information that is specific to processing unit 16. Memory 20 stores an ID code that is set in PID 6 by the manufacturer. The ID code of a device, which may be the device serial number, is unique to each device. Memory 20 also stores a fingerprint template that is generated by processing unit 16 from a fingerprint image signal provided by optics 12 unit when an individual first enrolls into PID 6, as will be described in detail below. That fingerprint image signal is representative of an image of a fingerprint of the enrolled individual. The fingerprint template is a data set that is representative of features of the enrolled individual's fingerprint. The fingerprint template is normally not changed once it is established in memory 20. In some embodiments, PID 6 may include a serial port (not shown), which can be used to plug into a computer to update or change the fingerprint template. For security purposes, PID 6 would be used to perform an identification verification before allowing such a change.

Processing unit 16 also includes an encryption algorithm incorporated into an encoder 23. In the embodiment illustrated in FIG. 1, the encryption algorithm is programmed into processor circuit 18. A private key that is stored in memory 20 is used with the encryption algorithm for encryption. The private key can be set into memory by the manufacturer, and is specific to each PID 6. Different PIDs 6, which have different processing units 16, will typically have different private keys. The encryption algorithm, on the other hand, can be the same for all PID's 6.

Host facility 4 is part of a host system 30. Host system 30 will typically be bank ATM systems, point of sale systems, and the like. Host system 30 also

includes a host processing unit 32, which has a processor circuit 34 and memory 36. Communication unit 8 in host facility 4 includes a receiver module 38 and a transmitter module 40. Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42.

Memory 36 stores ID codes of enrolled individuals who have registered with host system 30. Memory 36 also stores public keys associated with respective ones of the stored ID codes. By employing the correct public key associated with a specific ID code, host processor circuit 34 can decrypt a signal that has been encrypted according to the encryption algorithm and personal key associated with the specific ID code, in a manner known in the encryption arts. The public key can also be stored with a trusted third party 39, which provides this service for several host systems in a known manner.

Signals 41 may be transmitted between PID 6 and host facility via any wireless transmission method. Transmission can be via RF, infrared, induction, sound, or the like. In this embodiment, PID communication unit 24 and host communication unit 8 will normally have a short transmission range of approximately a meter or less, however, longer ranges can be used as well. Hard-wire transmission methods can also be employed, either alone or in combination with a wireless transmission method. For example, transmission can employ dial tone modulation frequency (DTMF)(tone transmission) via a conventional phone system, employ a cable TV line in conjunction with the cable remote control system, or employ a computer communication medium, such as the Internet or a private network. PID 6 can employ more than one transmission/reception mode, such as, for example, an RF and a DTMF unit.

In another embodiment of a security system 2A, shown in FIG. 2, a PID 6A includes most of the features of PID 6 described above with reference to FIG. 1, with some significant differences. Note that features that system 2 has in common with system 2A are labeled with the same reference numerals in FIGS. 1 and 2, which convention is continued in the remainder of the FIGS. and in the following description. One difference is that communication module 24A lacks receiver module 26. Also, encoder 23A includes an encoder chip, for example, the HSC200

or HSC300 KEELOQ® Code Hopping Encoder, available from Microchip Technology, Inc. of Chandler, Arizona, that contains the encryption algorithm. Security system 2A includes a host facility 4A in which host processing unit 32A is located at the same site as host facility 4A. Host system communication unit 8A includes a receiver module 38, but does not include a transmitter module.

The embodiment illustrated in FIG. 2 will typically be employed with systems such as garage door openers, automobile security systems, door locks, and the like. As such, PID communication module 24A will have a longer transmission range than communication module 24 in the embodiment illustrated in FIG. 1.

Encoder 23A includes an ID code, which may be a serial number of encoder 23 or PID 6A. Encoder 23A also includes a synchronization counter, an encryption key and an encryption algorithm that employs the encryption key. Host system 4A must "learn" the ID code and the synchronization counter for each PID 6A which is used to access a function of host system 4A. Host system 4A must also know the encryption key.

Referring now to FIGS. 4A-4D, one embodiment of a PID 6B, which includes all the features also shown in FIG. 1, includes a housing 44 similar in size to a personal pager or a small cellular telephone. A front side 46 includes a keypad 48 for entering data and commands, and a liquid crystal display 50 for displaying data being entered with keypad 48 and for displaying status signals to the user. Keypad 48 can be eliminated in some models where programmability is not required. Platen 15 is located at the top of PID 6B, and is contoured for a finger. Platen 15 is also slightly recessed in housing 42 to provide some protection from scratching. A back side 56 of PID 6B includes a battery cover (not shown) and apertures for a DTMP speaker (not shown). A serial port can be included under the battery cover.

Housing 42 includes a slot 52 for receiving a smart card 54, which is shown in shadow being fully inserted into slot 52 in FIG. 4A. Smart card 54 includes external memory 20, and can be removed from one housing 42 and used in a new housing 42. Because memory 20 contains all the personal information, i.e., the private key, the ID code, and the fingerprint template, the smart card can be used with a different PID housing 42 without having to re-enroll the user or re-register

any user information with host systems. Some models in which memory 20 is hard-wired inside housing 42 would not include smart card slot 52.

FIGS. 5A and 5B illustrate an embodiment of a PID 6C in which keypad 48 and smart card slot 52 are not included. PID 6C does, however, include platen 15, display 50, and a belt clip 58, which could be included in any model.

FIG. 6 illustrates an embodiment of a PID 6D which is structured similar to the embodiment illustrated in FIG. 2, for uses such as a garage door opener or automobile security system. PID 6D includes platen 15 at the top of housing 42, and three function buttons. For an automobile security system the function buttons can be a driver door button 60, a trunk button 62 and an alarm button 64. Buttons 60, 62, and 64 can be adapted for use with other host systems having different functions.

Optics unit 12 can be an image sensor module available from Fingerscan PTY Ltd (an Identix company), of Sydney, Australia, as part of their F3 OEM Kit. The entire F3 OEM Kit manual, published in 1998, is incorporated herein by reference. Platen 15 and imaging device 14 have a usable area of about 16 mm X 18 mm. Imaging device 14 in the F# OEM kit is a CMOS device that provides a video output comprising an analog fingerprint image signal representing an image of a finger placed on platen 15. The fingerprint image signal is communicated to processing unit 16 via a six-wire connector 68, which is shown in a circuit diagram illustrated in FIG. 9.

Most of processing unit 16 is also included in the F3 OEM Kit. Referring again to FIG. 9, processor circuit 18 includes an SH7034 32-bit RISC microprocessor 70, made by Hitachi of Japan. Microprocessor 70 communicates over an 8-bit data bus 72 with external memory 20 and A/D 22, and over control lines 74, 76 with optics unit 12. The SH7034 microprocessor 70 has a 64 Kb internal programmable read only memory (PROM) engine and an internal 4 Kb static random access memory (SRAM).

In the PROM resides a Fingerscan Biometrics Engine (FBE), which includes algorithms for capturing and processing fingerprint image signals. These algorithms allow a finger image of approximately 140 Kbytes to be converted into a finger model, or template, of approximately 120 bytes. This size saves memory

and improves the speed of processing by decreasing the time it takes to transfer finger models to and from the internal memory. The FBE includes special instruction sequences to optimize the following operations: image capture and background rejection; video signal filtering and digitizing; template matching; finger presence detection; false finger detection; and power on self test.

A/D 22 converts the analog video signal from optics unit 12 into digital data that is stored in memory for subsequent use by processor circuit 18. Memory 20 also stores the finger template of the user who is enrolled in PID 6, and also stores custom written code. Microprocessor 70 controls and has access to 1 Mbyte in DRAM 78 -70) and 512 Kbytes of external flash memory in PROM 80. DRAM 78 includes two NEC 424400 chips, and PROM 80 is an AMD 29F040 chip.

In one embodiment of communication unit 24, transmitter module includes an induction loop data link, which is configured as a short-range (< 0.5 m) wireless modem, operating at 1200 Baud, at 70 KHz carrier frequency, using amplitude shift keying modulation. The protocol is half duplex, carrier detect multiple access (modified aloha) and the software includes a CRC 16 packet error correction method. A processor included in transmitter module is based on a PIC16C72 device. The transmit current is typically 1 mA.

In the embodiment illustrated in FIG. 9, encoder 23 resides in code programmed into processing circuit 18. However, as discussed above, other embodiments may base encoder 23 on a dedicated encoder chip, such as the HSC200 or HSC300 KEELOQ® Code Hopping Encoder. A PID may include encryption code residing in processor circuit 18 and also include an encoder chip so that PID can combine the functions of the embodiments illustrated in FIGS. 1 and 2 in a single unit. These encoder chips combine a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28-bit serial number and 6 information bit to create a 66-bit transmission stream. The length of the transmission eliminates the threat of code scanning, and the code hopping mechanism makes the transmission unique, thus rendering code capture and resend schemes useless.

An owner of PID 6 must first "enroll" into the unit. Enrollment is the process of scanning a finger to create an image which is stored as a fingerprint template in memory 20. The user enrolls on the unit by removing the "packing"

cover and placing a thumb or finger on platen 15. PID can be configured to automatically start the enrollment routine with this action. Enrollment takes approximately 7 seconds. The resultant template is stored in memory 20. Ideally, PID 6 is configured to enable a user to enroll one finger on each hand so that, if the user injures the finger they usually use for verification, an alternate image is available.

Enrollment preferably permits the user several attempts to check and test the operation on the verify. Instructions and queries would be indicated, for example, by display 50 in this mode (see FIG. 4A). Until the user accepts the enrollment the unit will not transmit signals in any way but will allow any number of attempts to re-enroll and verify (test) the operation. Once committed there is no going back or editing.

If the enrollment is be stored on a removable smart card 54 (see FIG. 4A) along with the ID code and private encryption key files, these would not be accessible to other devices. It allows users to swap their PID 6 and retain their enrolled identifying data on smart card 54, while using other PIDs 6. This is the same process used in digital portable telephones today. A user can take the SIM card out of the telephone and swap phones without any security issues.

Verification is carried out when a user places his finger on platen 15, or presses a verify button if included in PID 6. In the embodiment illustrated in FIG. 4A, the verify button can be a dedicated button, such as the # button 55, or could be any other button or sequence of buttons. Each time the user places his or her finger on platen 15 (or presses the verify button and places their finger on platen 15) the optics unit 12 creates a fingerprint signal indicative of the fingerprint image of the user's finger on platen 15. The fingerprint signal is compared to the stored fingerprint template. If the two are significantly similar, the user's identity is verified to be the enrolled person. Verification takes about 1 second or less once the fingerprint template has been retrieved from storage. The user's fingerprint is always verified with the fingerprint template to allow the use of the encryption key.

In programmable PID's, verification for individual users can be set at various threshold levels to account for users who may have very fine, worn or

damaged fingers. In this event the ease of use can be enhanced by reducing their verification threshold. Verification threshold can be set at the time of enrollment.

Once the owner or person controlling the unit is enrolled, the unit can then be "registered" with numerous organizations. The host organization is only interested in knowing the ID code and the public encryption key.

The operation of security system 2 illustrated in FIG. 1 is different from the operation of security system 2A illustrated in FIG. 2. The operation of the embodiment illustrated in FIG. 1 will be described first.

In the first embodiment illustrated in FIG. 1, each of PID 6 and host facility 4 include transmit and receive functions. A communication from PID 6 to host system 30 is encrypted according to an encryption algorithm that employs a private key in encrypting and a public key to decrypt. The public encryption key is associated with PID 6 and therefore also with the enrolled person. The private encryption key is stored or loaded into PID 6 at registration time or at manufacture. When a user registers with each host system 30, the user provides the user's ID code and public key to host facility 4 as part of the user's account record. The public key can be stored by the host system. Alternatively, the user provides the public key to a central authority (trusted third party 39) with which host system 30 can communicate.

Referring now to FIG. 7, a user of PID 6 approaches host facility 4, e.g., an ATM (100). As PID 6 reaches the range of the host facility's receiver module 38, the microprocessor is "powered up." The user may have to select a transmission mode that matches that of host system 30, if more than one transmission mode is available on PID 6. Processor circuit 18 causes transmitter module 28 to transmit the ID code signal without encryption (102). This is received by host receiver module 38 and passed on to host processing unit 32 (104). Host processing unit 32 verifies that the received ID code signal represents a registered ID code (106). If the verification fails, then the access process ends (108). If the ID code is verified, then the account or user information is located, including the public encryption key associated with the registered ID code (110). The public encryption key may have to be retrieved from a remote source, such as a central authority. A large random number is also generated by host processing

unit 32 (112), and is passed on to transmitter module 40. Transmitter module 40 transmits a random number signal indicative of the random number to PID 6 (114). Receiver module 26 passes the random number signal to processing unit 16 (116). PID 6 performs a user verification (118). If the verification fails, the process ends (108). Alternatively, PID 6 can display a prompt to try again. If the user's identity is successfully verified as a match with the enrolled person based upon a comparison of the stored fingerprint template and a fingerprint image signal generated when the user places his finger on platen 15, the private encryption key associated with PID 6 is used to encrypt the random number according to an encryption algorithm (120). Processing unit 16 causes transmitter module 28 to transmit a signal representing the encrypted random number to host system 30 (122), where host processing unit 32 uses the public encryption key to decrypt the encrypted random number (124). Host processing unit 32 then determines if the decrypted random number matches the random number (126). If this is successful, then the user is granted access to the host facility (128). If this verification fails, the user is denied access (108). The step of verifying the identity of the user with the biometrics (118) can be performed at other junctures of the process, such as prior to transmitting the ID code signal (102), however, it must be carried out before encrypting the random number (120).

Hardware for host system 30 can include a small communication unit 8 with a sensor, such as an RF antenna. Processor circuit 34 can include a CPU to generate a random number, to verify the ID code received from PID 6, to decrypt the encrypted random number received from PID 6, and to compare the decrypted random number with the earlier generated random number.

As these transmissions are random, there is no possibility of scanning or tracking the codes other than to find the original ID code, which is effectively of no real use. The random number generators are such that they will always produce unique codes.

If a host system 30, such as a bank, a store, or a credit card company, implements this system, it would have the users register by presenting themselves with their PID 6 and the required personal identification papers, which is no different than current methods of obtaining a bank card to access accounts with an

ATM. The bank or other host system 30 would ask the user to complete a verify on their PID 6 and read the ID code and test the send and receive of the encryption codes. This would establish the public key with the bank and confirm the private key in PID 6. The user is now ready to use the system. Note that the bank does not have the user's fingerprint template--it only has the ID code and the public encryption key. Therefore there is no privacy issue regarding release of the user's fingerprint template.

After the user registers, verification is as described above. From the bank's point of view, the ATM (for example) commences normal operation. The user, instead of entering a bank card and a personal identification number (PIN), may simply press a verify pad or button on their PID 6 while placing their finger on platen 15. The ATM receiver reads the ID code, and if the code is valid generates a large random number, and transmits the number to the user's PID 6. If the validation is successful, PID 6 then encrypts the random number using the private encryption key according to the encryption algorithm, and transmits the result back. The bank system checks the result using the public encryption key and confirms the correct identity of the user. The transaction proceeds.

The bank's ATM will typically be connected to the Bank central system via network 42. Network 42 can be used for transmitting signals between the ATM and the bank central system where the CPU and data bases may be located.

The private encryption key can only be used after a verify, host system 30 knows the ID is correct as the key is unique to that user. Therefore, only that user could be carrying the reader. The key may well be installed during manufacture but only released after the unit is loaded with a template.

In a second mode of operation, typically used in car alarm systems and the like, PID 6A is configured as shown in FIG. 2 to transmit, and host facility 4A is configured to only receive. Receiver module 38 is a standard automobile or garage door type of installation. There is no special adaptation other than the required alarm or immobilizer installation. These systems include a "learn" mode, which is used to program in the new system. In learning a registering person's PID 6A, the host system 4A learns the ID code, the synchronization counter timing, and the encryption key of that PID 6A. This process is essentially the same as the learning

process for many current model garage door openers, automobile security systems and the like.

Referring to FIG. 8, to obtain access to host facility 4A, the user activates PID 6A by placing a finger on platen 15. PID 6A performs a user verification from the internally stored fingerprint template (200). If the verify succeeds, processing unit 16A causes encoder 23A to generate an encrypted signal (202). If not successful, the process ends (204). The encrypted signal includes the unencrypted ID code of PID 6, encrypted synchronization counter information and unencrypted function button information. The encryption employs the encryption key resident in encoder 23A. Transmitter unit 28 then transmits the encrypted signal to host facility 4A (206). Host facility 4A than passes the encrypted signal to host processing unit 32A, which checks the ID code for a match with the ID code of a registered user (208). Typically, there will be only a small number of registered users for car lock and garage door systems, and each may have the same ID code and encryption key. If there is no match, then the process ends (204). If there is a match, host processing unit 4A retrieves the stored encryption key and decrypts the encrypted portion of the received encrypted signal (210). Host processing unit then verifies that the synchronization counter information in the decrypted signal matches stored synchronization counter information in memory 36 (212). If the synchronization counter information does not match the stored information, then the process ends (204). If the synchronization counter information matches the stored information, then the user is granted access to host facility 4A (214). The access granted is determined by the function button information contained in the encrypted signal.

In both embodiments, the PID unit can be set in a low power "StandBy" or "Off" function, or could be powered on by the action of pressing the platen.

There are a large number of alternative applications. For example, a hotel could employ the invention in a door lock security system. A hotel registrant would register his PID with the hotel. The hotel would identify the user's ID code to the lock on his room's door. A member of the hotel staff would carry a master PID which would configure the door to that PID and some other master PID for

hotel staff. There would be no need for a hard wired communications system to each door unless central control is required.

The biometric sensor 11 may include a direct contact device instead of an optic sensor unit 12. Direct contact capacitive chip fingerprint sensors can be obtained from SGS Thomson Microelectronics, of Phoenix Arizona, from Veridicom, Inc., of Santa Clara California, and from Harris Semiconductor, of Melbourne, Florida. A direct contact thermal sensor may also be used for fingerprint sensing.

Other embodiments are within the scope of the claims.

For example, referring to FIGS. 10A and 10B, a PID 300 is configured to identify a user of a vehicle, provide immobilization security for the vehicle, and to automatically maintain a log of vehicle travel information. PID 300 is configured as a hand-held device with a finger platen 301, a display 302, an input keypad 304, and an input/output port 306. Input/output port 306 plugs into an in-vehicle adaptor module 307 which couples PID 300 to the vehicle power system 308, the engine management computer 310 and a global positioning system (GPS) 312. Adaptor module 307 includes a unique identification number that relates to the registration details of the vehicle. To operate the vehicle, the user must first be enrolled in PID 300 and PID 300 must be inserted into adaptor module 307. To start the vehicle, the user must activate a start-up option on PID 300 and must press (or swipe) a finger against finger platen 301. PID 300 extracts a representation of the user's fingerprint and compares the extracted information with a stored representation of the user's fingerprint. If the two fingerprint representations substantially match, PID 300 transmits a verification signal that enables the user to access the engine management system and operate the vehicle. After the user's identity has been verified, PID 300 begins to log trip information, including start time, vehicle location and trip log (map) information based on information received from GPS 312, vehicle speed and distance traveled. There is no need for the user to log travel information because all logging information is automated. The user may, however, enter additional information into PID 300 through keypad 304. PID 300 is programmable. For example, PID 300 may be programmed to prompt the user to enter additional identification information at

different times during a trip or at preselected vehicle locations based upon signals received from GPS 312. PID 300 includes a transceiver (e.g., an RF transceiver or a digital cellular telephone transceiver) that enables the device to be interrogated remotely (e.g., by devices located at preselected vehicle checkpoint locations, such as the locations of existing highway monitoring cameras).

Referring to FIG. 11, in another embodiment, a PID 320 is configured as a pocket-sized unit which may be clipped to a pocket 321 of a user's shirt and is configured to provide access to a secure location. The housing of PID 320 includes a pocket for holding a user identification card 325 (e.g., a photo ID card). PID 320 includes a finger platen 322, a notification light 324 (e.g., a red light emitting diode), a processor, and a receiver. When the receiver is located near (e.g., within about 0.5 meters) the transmitter of a host system which controls access to the secure location, the processor switches from a low power operation (standby or off mode) to a normal power operation and causes notification light 324 to flash, prompting the user to press (or swipe) a finger against finger platen 322. PID 320 extracts a representation of the user's fingerprint and compares the extracted information with a stored representation of the user's fingerprint. If the two fingerprint representations are sufficiently close, PID 320 transmits a verification signal to the host system. Upon receipt of the verification signal, the host system grants access to the secure location and logs information relating to the user and time access was granted. PID 320 includes an RF transceiver which enables PID 320 to wirelessly receive enrollment information (e.g., add or remove users) and to set access codes for each of the enrolled users.

Still other embodiments are within the scope of the claims.

WHAT IS CLAIMED IS:

1. A portable, hand-held personal identification device for providing secure access to a host facility, comprising:

a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative thereof;

a processing unit responsive to the biometric signal, being adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person, and to provide a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person, wherein the verification signal is indicative of the enrolled person or the device; and

a communication unit, including a transmitter circuit, is adapted to transmit the verification signal to a remote host system.

2. The personal identification device of claim 1, wherein the biometric sensor system includes a fingerprint sensor.

3. The personal identification device of claim 2, wherein the fingerprint sensor includes a platen adapted for placing a finger thereon.

4. The personal identification device of claim 3, wherein the fingerprint sensor further includes an optical image sensor.

5. The personal identification device of claim 1, wherein the biometric sensor system includes an optical image sensor.

6. The personal identification device of claim 5, wherein the optical image sensor comprises a CMOS chip.

7. The personal identification device of claim 1, wherein the processing unit includes a processor circuit, a memory and an encoder, wherein the memory stores the biometric data, and wherein the verification signal comprises an encrypted signal encrypted by the encoder.

8. The personal identification device of claim 7, wherein the encoder comprises an encoding circuit, and wherein the verification signal further comprises an ID code indicative of the enrolled person or the device.

9. The personal identification device of claim 7, wherein the encoder comprises an encryption algorithm programmed into the processor, and wherein the encryption algorithm employs a private key indicative of the enrolled person or the device.

10. The personal identification device of claim 9, wherein the communication unit further comprises a receiver circuit, wherein the memory further stores an ID code indicative of the enrolled person or the device, wherein the processor unit is further adapted to first cause the transmitter circuit to transmit an ID code signal indicative of the ID code to the host system, wherein the receiver circuit is adapted to receive a host response signal transmitted by the host system in response to the ID code signal, and wherein the processor unit employs the encryption algorithm and the private key to encrypt the host response signal to create the verification signal, and causes the transmitter circuit to transmit the verification signal to the host system only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person.

11. The personal identification device of claim 7, wherein the memory is located in a removable plug-in module, the personal identification device further comprising a socket adapted to receive the module.

12. The personal identification device of claim 1, wherein the communication unit further includes a receiving circuit being adapted to receive a host response signal from the host system.

13. The personal identification device of claim 1, wherein the communication unit is adapted for remote communication with the host system via a wireless communication medium.

14. The personal identification device of claim 1, further comprising a display.

15. The personal identification device of claim 14, further comprising a keypad.

16. The personal identification device of claim 1,

wherein the biometric sensor system includes a fingerprint sensor and wherein the biometric trait is a fingerprint;

wherein the communication unit further comprises a receiver circuit adapted to receive signals transmitted by the host system;

wherein the processing unit includes:

memory for storing an ID code associated only with the device, a personal encryption key associated only with the device, and the biometric data;

a processor circuit adapted to encrypt the host response signal according to an encryption algorithm employing the personal encryption key;

wherein the processing unit is further adapted to first cause the transmitter circuit to transmit an ID code signal indicative of the ID code to the host system, wherein the receiver circuit is adapted to receive a host response signal transmitted by the host system in response to the ID code signal, and to employ the encryption algorithm and the private encryption key to create the verification signal by encrypting a host response signal received by the receiver circuit from the host system in response to the ID code signal.

17. The personal identification device of claim 16, wherein the memory is located in a removable plug-in module, the personal identification device further comprising a socket adapted to receive the module.

18. A portable, hand-held personal identification device for providing secure access to a host facility, comprising:

a housing;

a fingerprint sensor system capable of sensing a fingerprint of a user and providing a fingerprint signal indicative thereof, the fingerprint sensor system including a platen on a surface of the housing adapted to receive a finger;

a communication unit in the housing being adapted for wireless communication with a separate host system, including a transmitting circuit and a receiving circuit; and

a slot in the housing for receiving a smart card that includes a memory.

19. The personal identification device of claim 18, in combination with the smart card, wherein the memory in the smart card stores a fingerprint template representative of the fingerprint of an enrolled person, and an ID code and a personal encryption key being associated with the device, wherein the processing circuit is adapted to cause the ID code signal from memory to be transmitted by the transmitting circuit, and wherein the processing circuit is further adapted to cause a host response signal received by the receiving circuit signal from the host system in response to the ID code signal to be encrypted according an encryption algorithm employing the personal encryption key and to cause the encrypted host response signal to be transmitted by the transmitting circuit only if the fingerprint signal corresponds sufficiently to the fingerprint template to verify that the user is the registered person.

20. The personal identification device of claim 18, further comprising an alphanumeric display.

21. The personal identification device of claim 20, further comprising a keypad for inputting data.

22. A method of providing secure access to a host facility, comprising:

registering one or more persons with the host facility, including storing a unique ID code and a public encryption key for each registered person;

receiving a first transmission comprising a first user signal at the host facility;

generating and then transmitting a random number signal only if the first user signal represents one of the stored ID codes;

receiving a second transmission comprising a second user signal at the host facility;

decrypting the second user signal with the public encryption key associated with the registered person who is also associated with the stored ID code represented by the first user signal; and

providing access to the host facility only if the decrypted second user signal represents the random number.

23. A method of providing access to a secure host facility only to registered persons, comprising:

registering one or more registered persons with the host system, wherein registering each registered person includes storing an ID code associated only with a portable hand-held device under the control of that registered person;

transmitting an ID code signal from a portable hand-held device to a facility of the host system, wherein the ID code signal represents an ID code associated with the transmitting device;

generating, at the host facility, a random number signal representing a random number in response to the ID code signal only if the ID code signal is representative of the ID code of the device controlled by one of the registered persons;

retrieving, with the host system, a public key associated with the one of the registered persons only if the ID code signal is representative of the ID code of the one the device controlled by the one of the registered persons;

transmitting the random number signal from the host facility to the transmitting device;

receiving the random number signal with the transmitting device;

generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of the transmitting device;

comparing, with the transmitting device, the user fingerprint signal to a fingerprint template stored in the transmitting device, the fingerprint template representing a fingerprint image of a person who is enrolled with the transmitting device;

encrypting the random number signal with the transmitting device, the random number signal being encrypted according to an encryption algorithm employing a private key associated only with the transmitting device;

transmitting the encrypted random number signal from the transmitting device to the host facility only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person;

decrypting the encrypted random number signal with the host system, including employing the retrieved public key; and

providing the user access to the host facility only if the decrypted encrypted random number signal represents the random number.

24. The method of claim 23, wherein retrieving the public key includes retrieving the public key from a trusted third party.

25. The method of claim 23, wherein transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each includes transmitting via a wireless transmission.

26. The method of claim 23, wherein transmitting the ID code signal, transmitting the random number signal, and transmitting the encrypted random number signal each includes transmitting via at least one of a modem, a cable access TV line, and a computer communication medium.

27. A method of providing a secure function at a host facility only to a registered person, comprising:

registering a person with the host facility by storing an ID code associated only with a portable registered device controlled by the registered person, learning a synchronization counter of the registered device, storing an encryption key associated with the registered device and associating the encryption key of the registered device with the stored ID code;

generating a user fingerprint signal representing a fingerprint image of a user's finger being placed on a platen of a portable user device;

comparing, with the user device, the user fingerprint signal to a fingerprint template stored in the user device, the fingerprint template representing a fingerprint image of an enrolled person who is enrolled with the user device;

generating an access signal with the user device only if the fingerprint image represented by the user fingerprint signal corresponds sufficiently to the fingerprint image represented by the fingerprint template to verify that the user is the enrolled person, the access signal comprising an ID code associated only with the user device, button press information representing a requested function, and encrypted data encrypted with an encryption key associated with the user device, the encrypted data including a synchronization counter associated with the user device;

transmitting the access signal from the user device to the host facility;

determining, with the host facility, if the ID code in the access signal matches the stored ID code;

retrieving the encryption key of the registered device if the match is successful;

employing the encryption key of the registered device to decrypt the encrypted data and determine the synchronization counter of the user device;

comparing the synchronization counter of the user device with the synchronization counter of the registered device;

providing the requested function represented by the button press data only if the synchronization counter of the user device matches the synchronization counter of the registered device.

28. A method of accessing a secure host facility, comprising:

sensing a biometric trait of a user that is unique to a user with a biometric sensor system of a portable device, and providing a biometric signal indicative of the biometric trait;

comparing, with the portable device, the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person;

providing a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person; and

transmitting the verification signal and an ID code signal to a remote host system, wherein the ID code signal is indicative of an ID code associated only with the portable device, and wherein the host system provides access to the secure facility in response to the verification signal only if host facility determines that personal device associated with the ID code belongs to a registered person.

29. A personal identification system, comprising:

a biometric sensor configured to extract a representation of a biometric trait of a user;

a processor configured to verify the user's identity based upon a comparison of a representation of a biometric trait extracted from a user with a stored representation of the biometric trait; and

a transmitter configured to transmit a verification signal indicative of a successful verification of the user's identity.

30. The system of claim 29, wherein the processor is configured to process signals received from a global positioning system (GPS) receiver.

31. The system of claim 30, wherein the processor is configured to derive trip information from the signals received from the GPS receiver.

32. The system of claim 31, wherein the trip information includes the location of the GPS receiver.

33. The system of claim 32, wherein the processor is programmable to prompt the user for additional verification information when the GPS receiver is positioned at a particular location.

34. The system of claim 29, further comprising a user input configured to enable a user to enter trip information, and wherein the processor is configured to process information received from the user.

35. The system of claim 29, wherein the transmitter is further configured to transmit signals representative of stored trip information.

36. The system of claim 29, wherein the biometric sensor, the processor, and the transmitter are housed within a portable, hand-held housing.

37. The system of claim 36, further comprising an input device mounted inside a vehicle and coupled to the vehicle's power system, and wherein the input device is adapted to receive the verification signal from the transmitter and to enable the user to turn on the vehicle only upon receipt of the verification signal.

38. The system of claim 36, wherein the housing has the form of a pocket-sized security badge.

39. The system of claim 36, wherein the housing is configured to receive a graphical representation of the user.

40. The system of claim 29, further comprising an automatic door locking device coupled to a vehicle door and adapted to unlock the door upon receipt of the verification signal.

41. The system of claim 29, further comprising an automatic door locking device coupled to a vehicle trunk and adapted to unlock the trunk upon receipt of the verification signal.

42. The system of claim 29, further comprising a receiver, and wherein the processor is operable to switch the system from a low power operation to a normal power operation when the receiver receives a power-up signal from a host system.

43. The system of claim 29, further comprising a memory configured to store the representation of the biometric trait.

44. The system of claim 44, wherein the memory is housed within a portable housing separable from the biometric sensor, processor and transmitter.

45. The system of claim 29, wherein the biometric sensor is configured to extract a representation of the user's fingerprint.

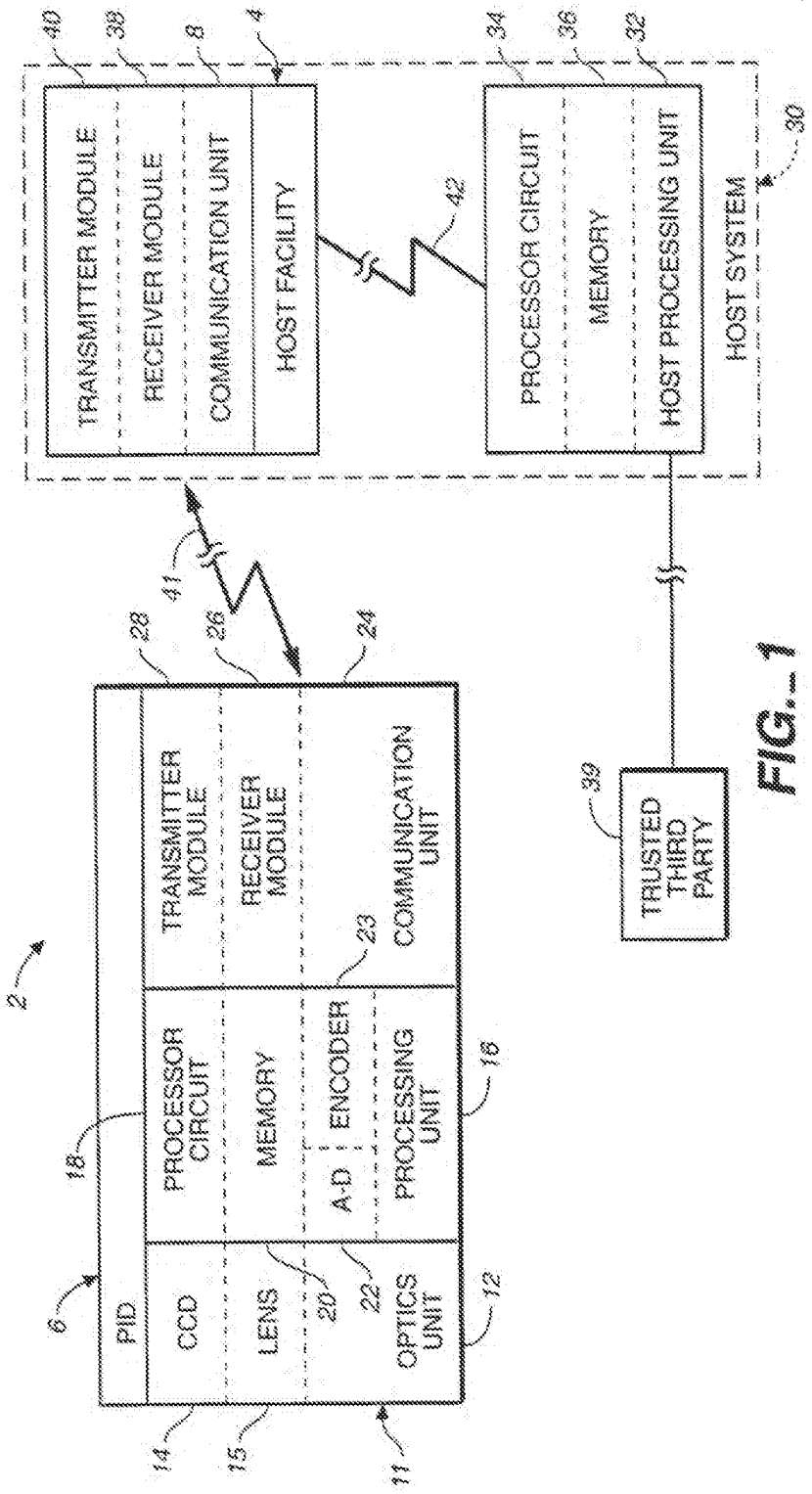

TRANSMITTER MODULE
RECEIVER MODULE
COMMUNICATION UNIT
HOST FACILITY
PROCESSOR CIRCUIT
MEMORY
HOST PROCESSING UNIT
HOST SYSTEM
TRUSTED THIRD PARTY
TRANSMITTER MODULE
RECEIVER MODULE
COMMUNICATION UNIT
PROCESSOR CIRCUIT
MEMORY
A-D
ENCODER
PROCESSING UNIT
PID
CCD
LENS
OPTICS UNIT
2
4
6
8
11
12
14
15
16
18
20
22
23
24
26
28
30
32
34
36
39
40
41
42

FIG._1

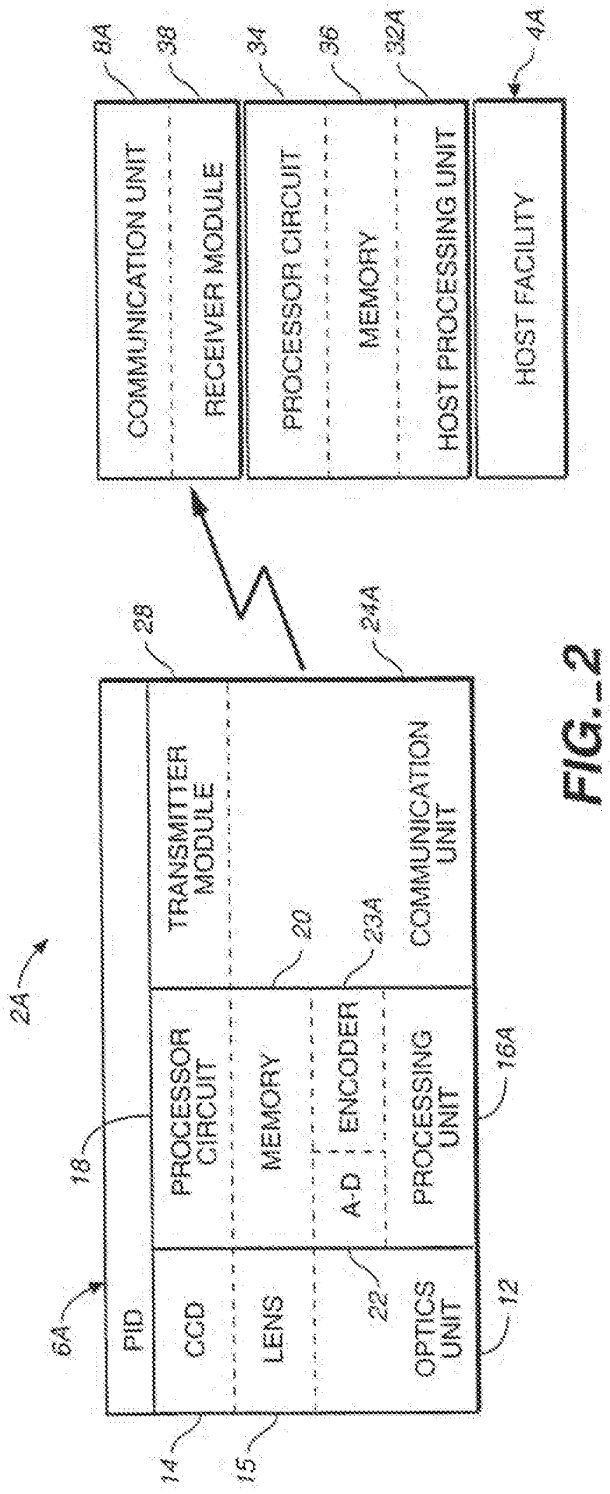

8A
38
34
36
32A
4A
COMMUNICATION UNIT
RECEIVER MODULE
PROCESSOR CIRCUIT
MEMORY
HOST PROCESSING UNIT
HOST FACILITY
28
24A
2A
TRANSMITTER MODULE
COMMUNICATION UNIT
20
23A
18
PROCESSOR CIRCUIT
MEMORY
A-D
ENCODER
PROCESSING UNIT
16A
6A
PID
CCD
LENS
22
OPTICS UNIT
12
14
15

FIG._2

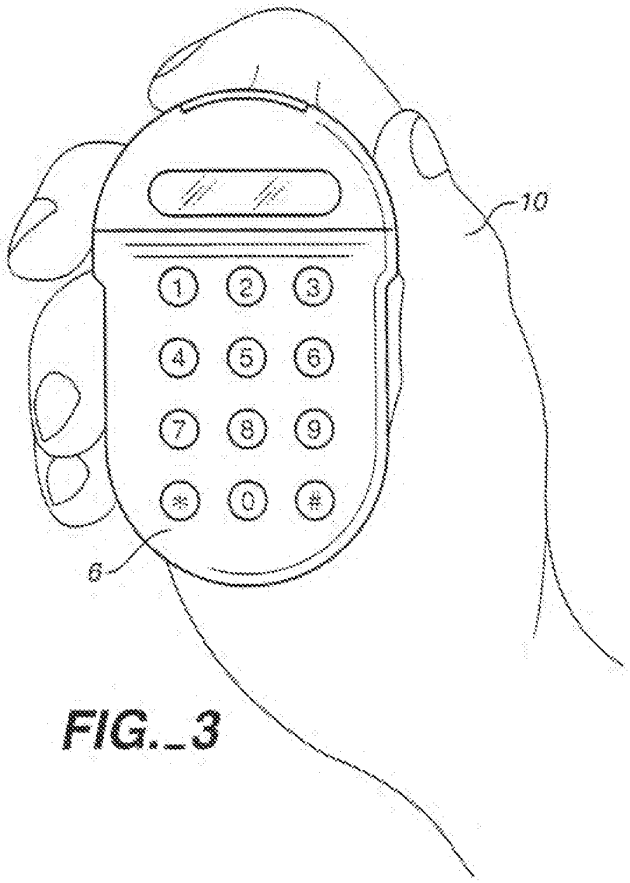


FIG._3

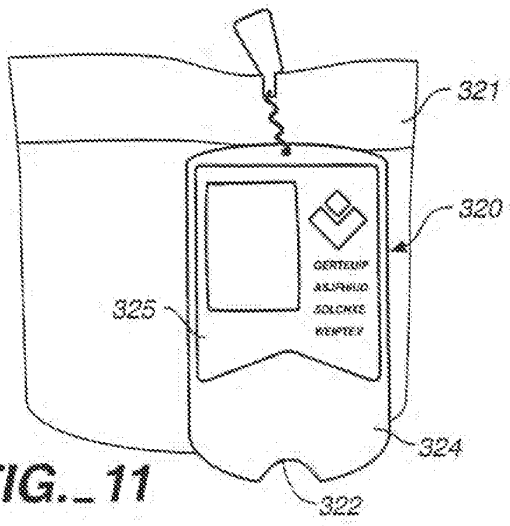


FIG._11

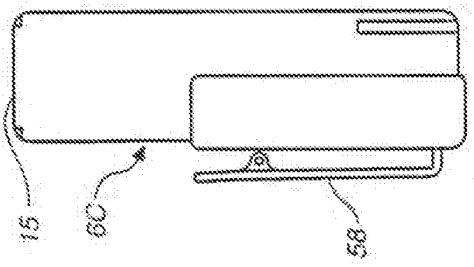


FIG._5B

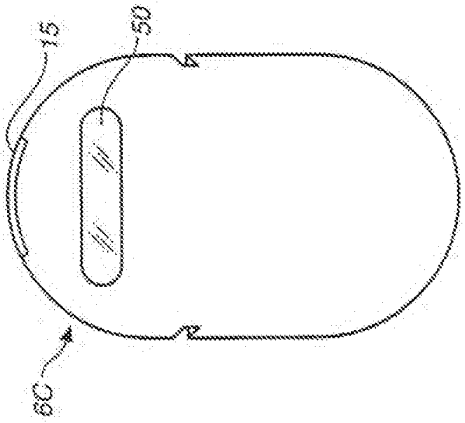


FIG._5A

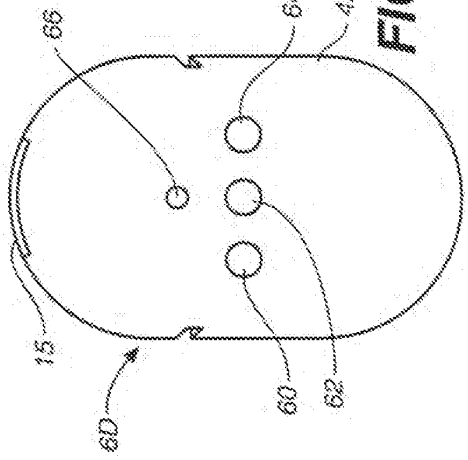


FIG._6

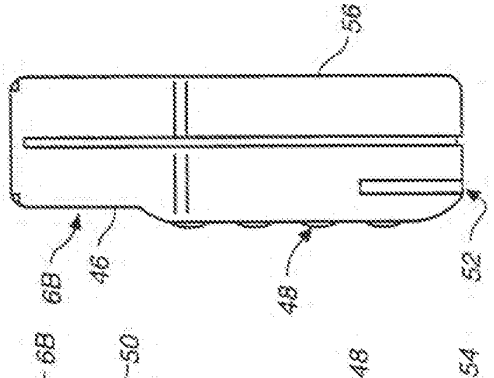


FIG._4B

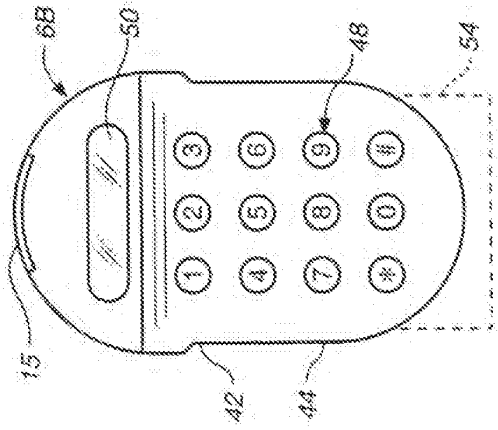


FIG._4A

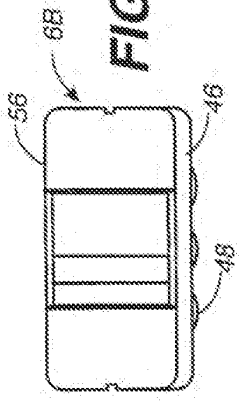


FIG._4C

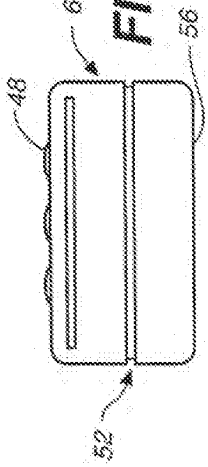


FIG._4D

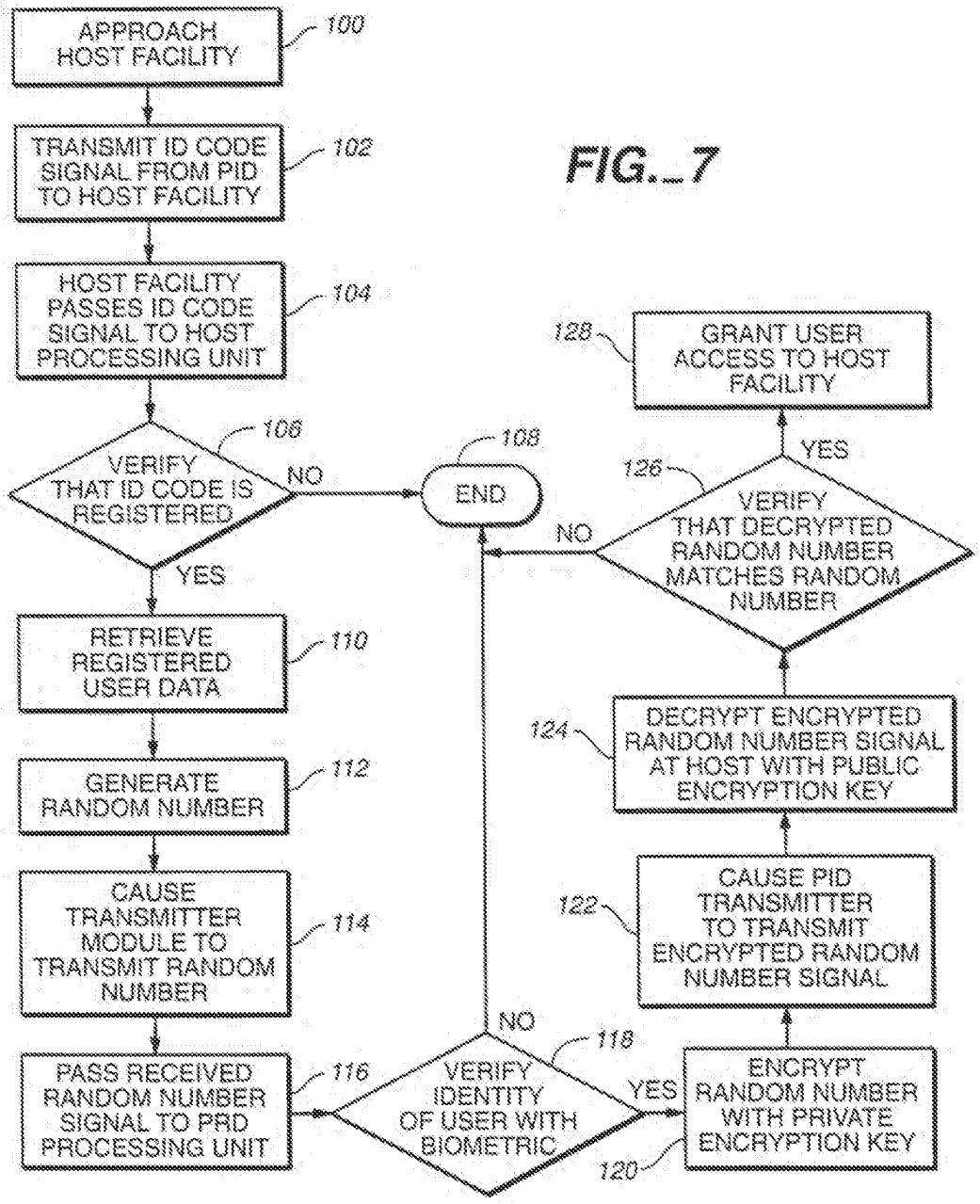

APPROACH HOST FACILITY
100
TRANSMIT ID CODE SIGNAL FROM PID TO HOST FACILITY
102
HOST FACILITY PASSES ID CODE SIGNAL TO HOST PROCESSING UNIT
104
VERIFY THAT ID CODE IS REGISTERED
106
NO
YES
END
108
RETRIEVE REGISTERED USER DATA
110
GENERATE RANDOM NUMBER
112
CAUSE TRANSMITTER MODULE TO TRANSMIT RANDOM NUMBER
114
PASS RECEIVED RANDOM NUMBER SIGNAL TO PRD PROCESSING UNIT
116
VERIFY IDENTITY OF USER WITH BIOMETRIC
118
NO
YES
ENCRYPT RANDOM NUMBER WITH PRIVATE ENCRYPTION KEY
120
CAUSE PID TRANSMITTER TO TRANSMIT ENCRYPTED RANDOM NUMBER SIGNAL
122
DECRYPT ENCRYPTED RANDOM NUMBER SIGNAL AT HOST WITH PUBLIC ENCRYPTION KEY
124
VERIFY THAT DECRYPTED RANDOM NUMBER MATCHES RANDOM NUMBER
126
NO
YES
GRANT USER ACCESS TO HOST FACILITY
128

FIG._7

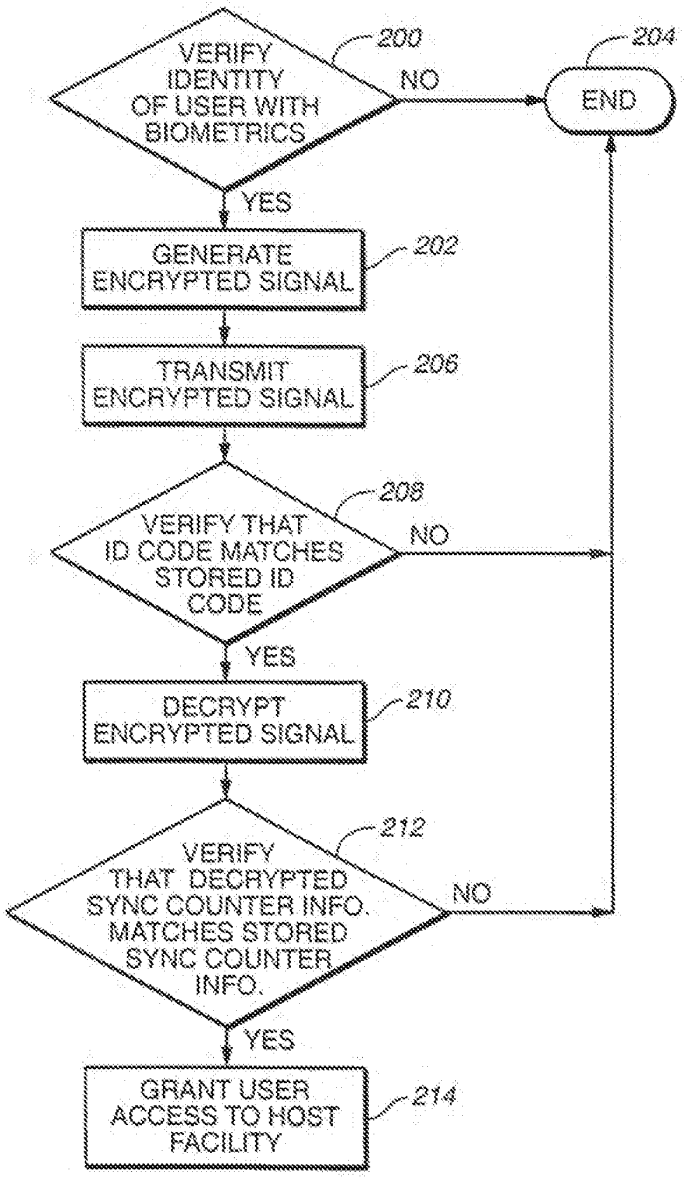

VERIFY IDENTITY OF USER WITH BIOMETRICS
200
NO
204
END
YES
GENERATE ENCRYPTED SIGNAL
202
TRANSMIT ENCRYPTED SIGNAL
206
VERIFY THAT ID CODE MATCHES STORED ID CODE
208
NO
YES
DECRYPT ENCRYPTED SIGNAL
210
VERIFY THAT DECRYPTED SYNC COUNTER INFO. MATCHES STORED SYNC COUNTER INFO.
212
NO
YES
GRANT USER ACCESS TO HOST FACILITY
214

FIG._8

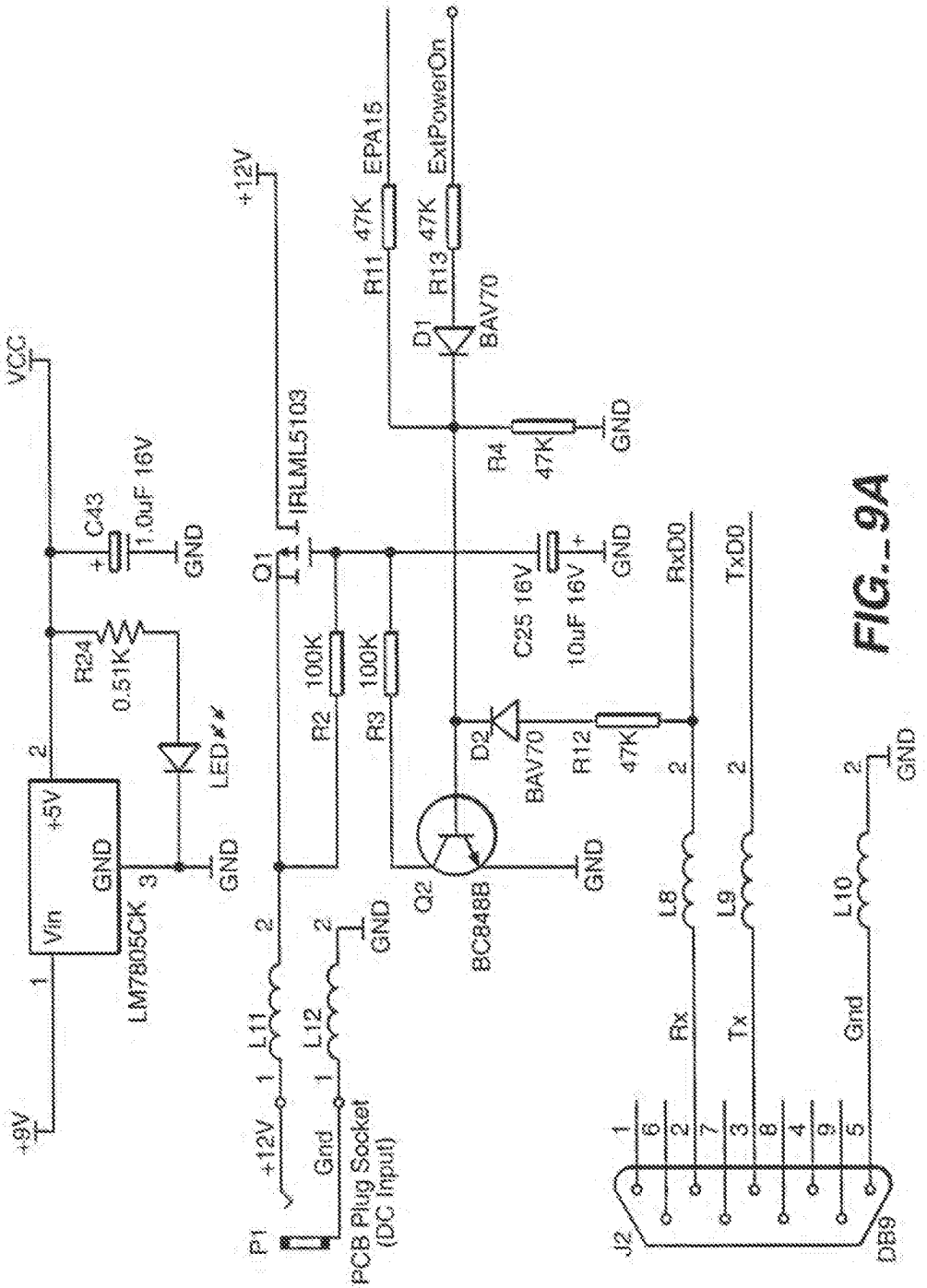

+9V
VCC
LM7805CK
Vin
+5V
GND
C43
1.0uF 16V
R24
0.51K
LED
P1
PCB Plug Socket
(DC Input)
+12V
Gnd
L11
L12
Q1
IRLML5103
R2
100K
R3
100K
Q2
BC848B
D2
BAV70
C25 16V
10uF 16V
R12
47K
R4
47K
D1
BAV70
R11
47K
R13
47K
EPA15
ExtPowerOn
RxD0
TxD0
L8
L9
L10
J2
DB9
Rx
Tx
Gnd

FIG._9A

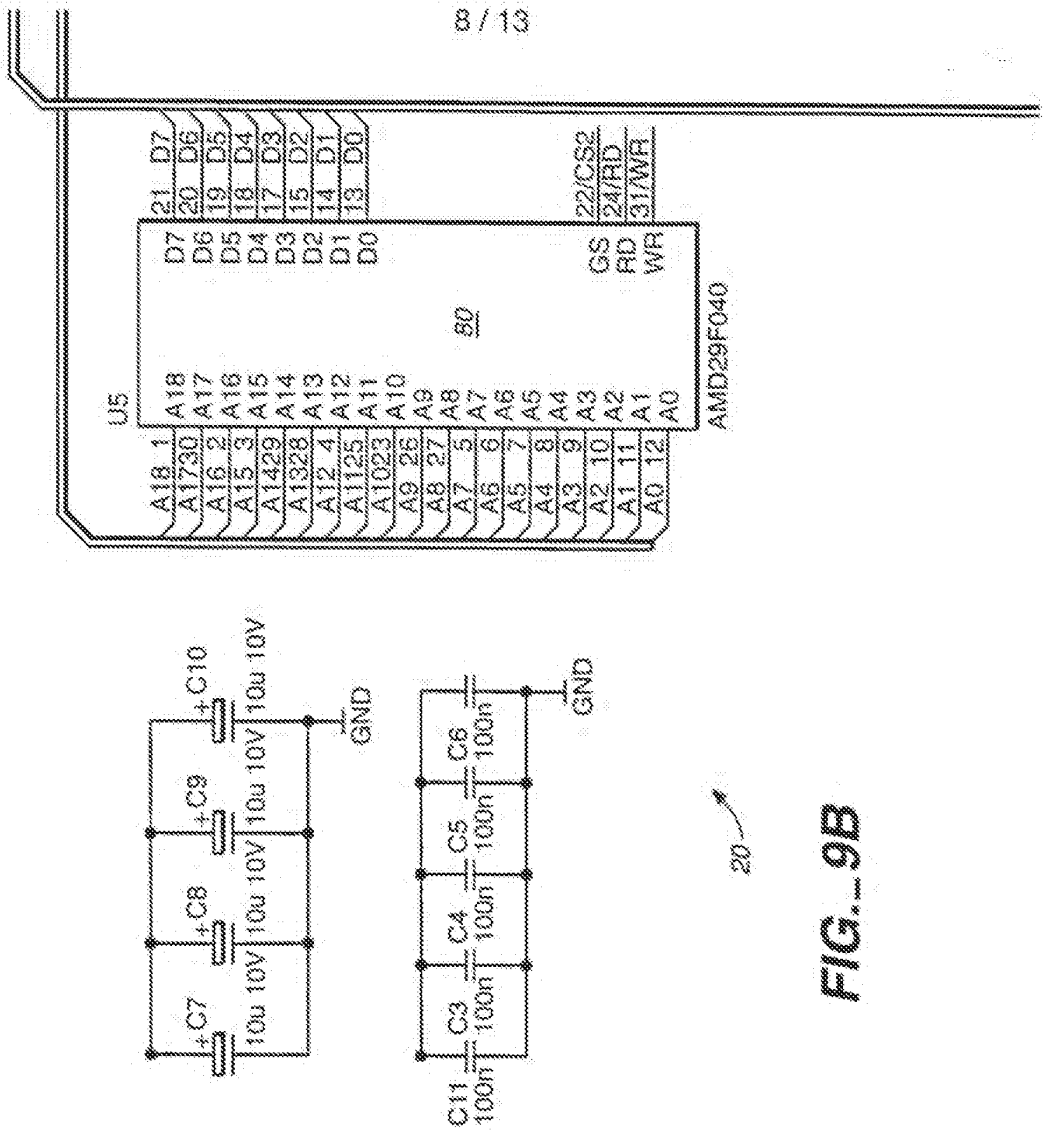

U5
AMD29F040
60
A18 1
A17 30
A16 2
A15 3
A14 29
A13 28
A12 4
A11 25
A10 23
A9 26
A8 27
A7 5
A6 6
A5 7
A4 8
A3 9
A2 10
A1 11
A0 12
D7 21
D6 20
D5 19
D4 18
D3 17
D2 15
D1 14
D0 13
GS 22/CS2
RD 24/RD
WR 31/WR
+C10 10u 10V
+C9 10u 10V
+C8 10u 10V
+C7 10u 10V
GND
C6 100n
C5 100n
C4 100n
C3 100n
C11 100n
GND
20

FIG._9B

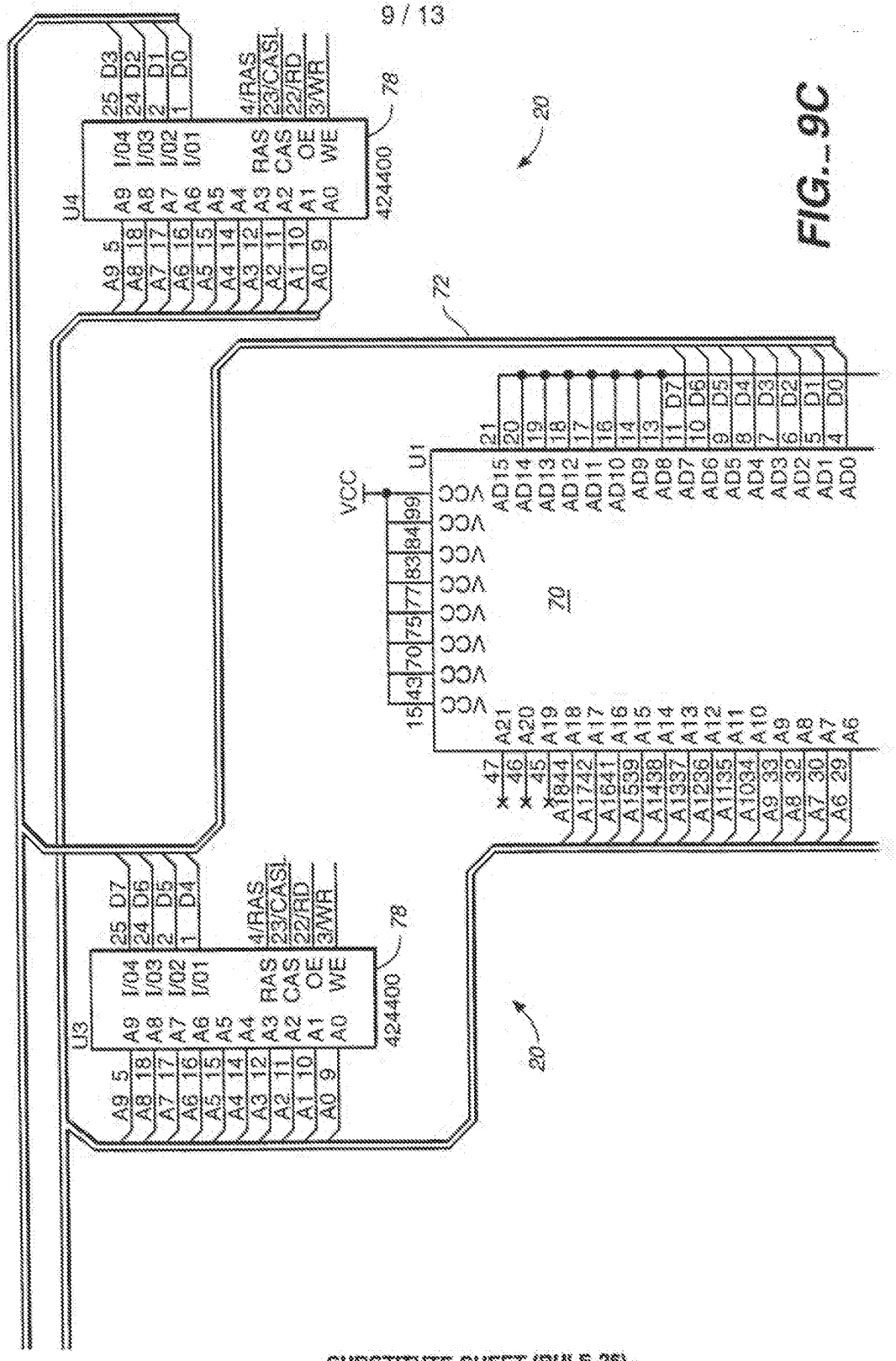

U4
U3
U1
424400
78
72
70
20
VCC
A9_5 A8_18 A7_17 A6_16 A5_15 A4_14 A3_12 A2_11 A1_10 A0_9
25 D3 24 D2 2 D1 1 D0
I/O4 I/O3 I/O2 I/O1
A9 A8 A7 A6 A5 A4 A3 A2 A1 A0
RAS CAS OE WE
4/RAS 23/CAS 22/RD 3/WR
25 D7 24 D6 2 D5 1 D4
15 43 70 75 77 83 84 99
VCC
21 20 19 18 17 16 14 13 11 10 9 8 7 6 5 4
AD15 AD14 AD13 AD12 AD11 AD10 AD9 AD8 AD7 AD6 AD5 AD4 AD3 AD2 AD1 AD0
D7 D6 D5 D4 D3 D2 D1 D0
47 46 45 44 42 41 39 38 36 35 34 33 32 30 29
A21 A20 A19 A18 A17 A16 A15 A14 A13 A12 A11 A10 A9 A8 A7 A6

FIG._9C

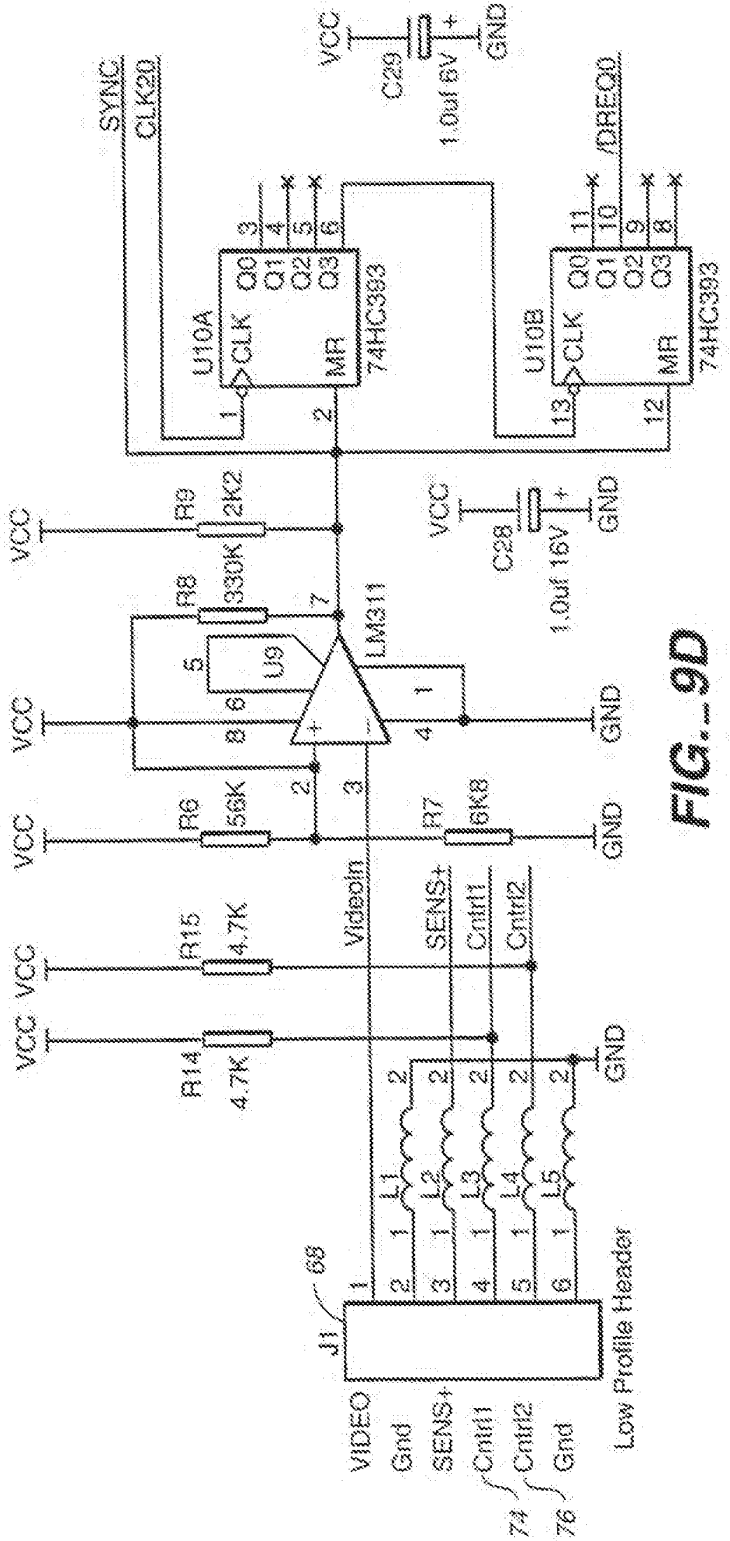

SYNC
CLK20
VCC
C29
1.0uf 6V
GND
U10A
74HC393
U10B
74HC393
/REQ20
R9
2K2
R8
330K
U9
LM311
C28
1.0uf 16V
R6
56K
R7
6K8
R15
4.7K
R14
4.7K
Videoin
SENS+
Cntrl1
Cntrl2
J1
68
L1
L2
L3
L4
L5
VIDEO
Gnd
SENS+
Cntrl1
Cntrl2
Gnd
74
76
Low Profile Header

FIG._9D

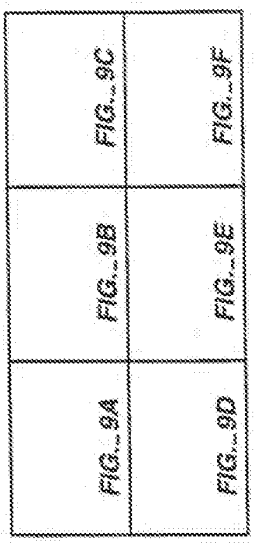

FIG._9A
FIG._9B
FIG._9C
FIG._9D
FIG._9E
FIG._9F

FIG._9

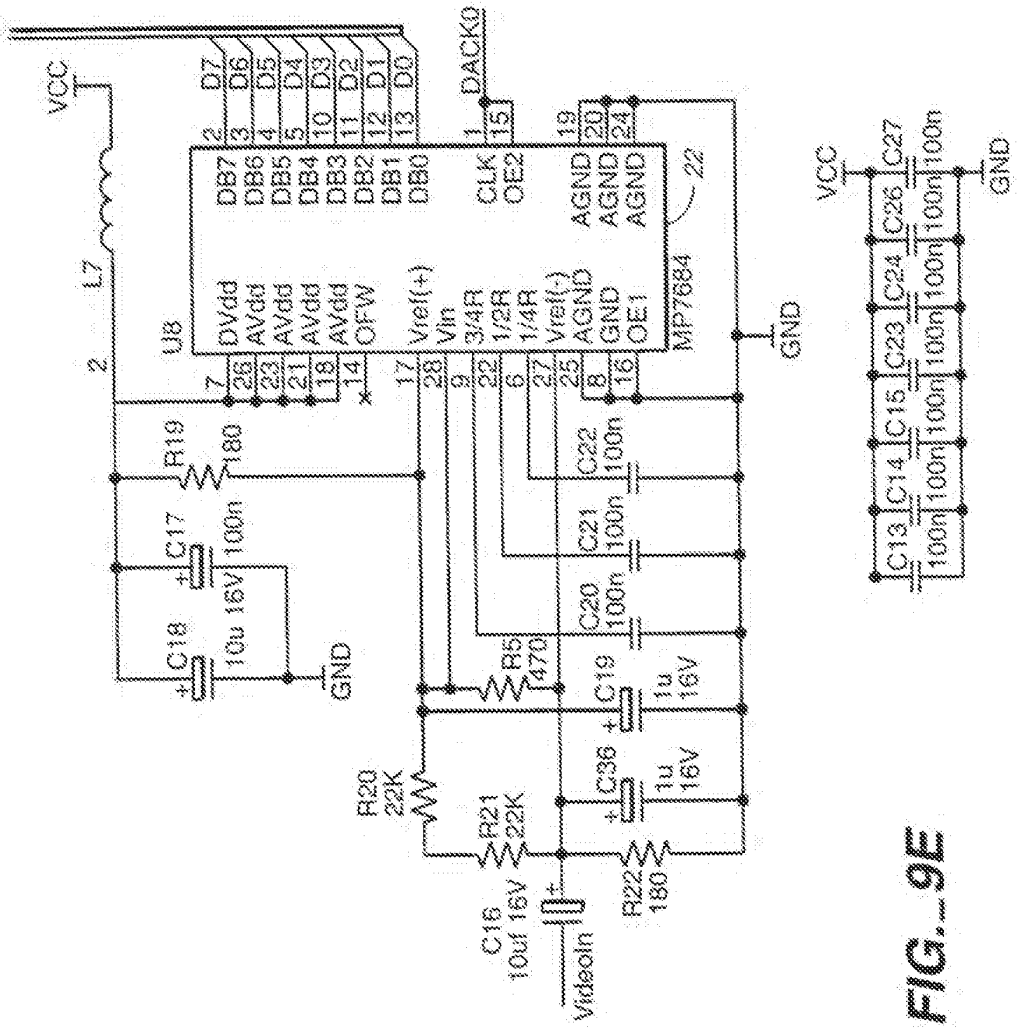
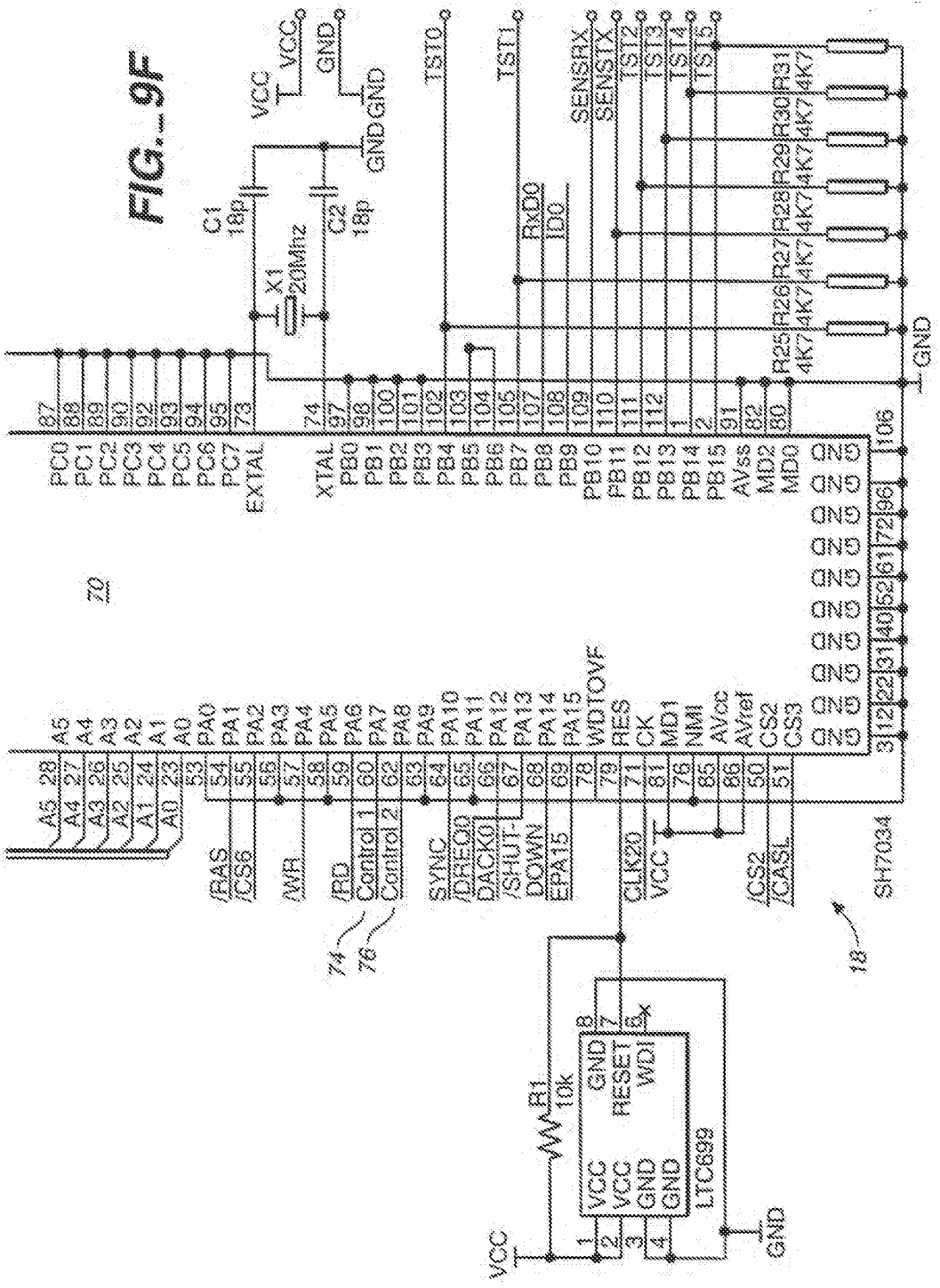

VCC
L7
2
U8
DVdd
AVdd
AVdd
AVdd
AVdd
OFW
Vref(+)
Vin
3/4R
1/2R
1/4R
Vref(-)
AGND
GND
OE1
MP7684
22
DB7
DB6
DB5
DB4
DB3
DB2
DB1
DB0
CLK
OE2
AGND
AGND
AGND
DACK0
D7
D6
D5
D4
D3
D2
D1
D0
R19
180
C17
100n
C18
10u 16V
GND
R5
470
C22
100n
C21
100n
C20
100n
C19
1u
16V
C36
1u
16V
R20
22K
R21
22K
R22
180
C16
10uf 16V
VideoIn
GND
VCC
C27
C26
C24
C23
C15
C14
C13
100n
GND

FIG._9E

FIG._9F


70
SH7034
18
74
76
C1 18p
C2 18p
X1 20Mhz
VCC
GND
TST0
TST1
SENSRX
SENSTX
TST2
TST3
TST4
TST5
RxD0
TD0
R1 10k
LTC699
GND
RESET
WDI
VCC
PC0
PC1
PC2
PC3
PC4
PC5
PC6
PC7
EXTAL
XTAL
PB0
PB1
PB2
PB3
PB4
PB5
PB6
PB7
PB8
PB9
PB10
PB11
PB12
PB13
PB14
PB15
AVss
MD2
MD0
PA0
PA1
PA2
PA3
PA4
PA5
PA6
PA7
PA8
PA9
PA10
PA11
PA12
PA13
PA14
PA15
WDTOVF
RES
CK
MD1
NMI
AVcc
AVref
CS2
CS3
/RAS
/CS6
/WR
/RD
Control 1
Control 2
SYNC
/DREQ0
/DACK0
/SHUT-DOWN
EPA15
CLK20
/CS2
/CASL

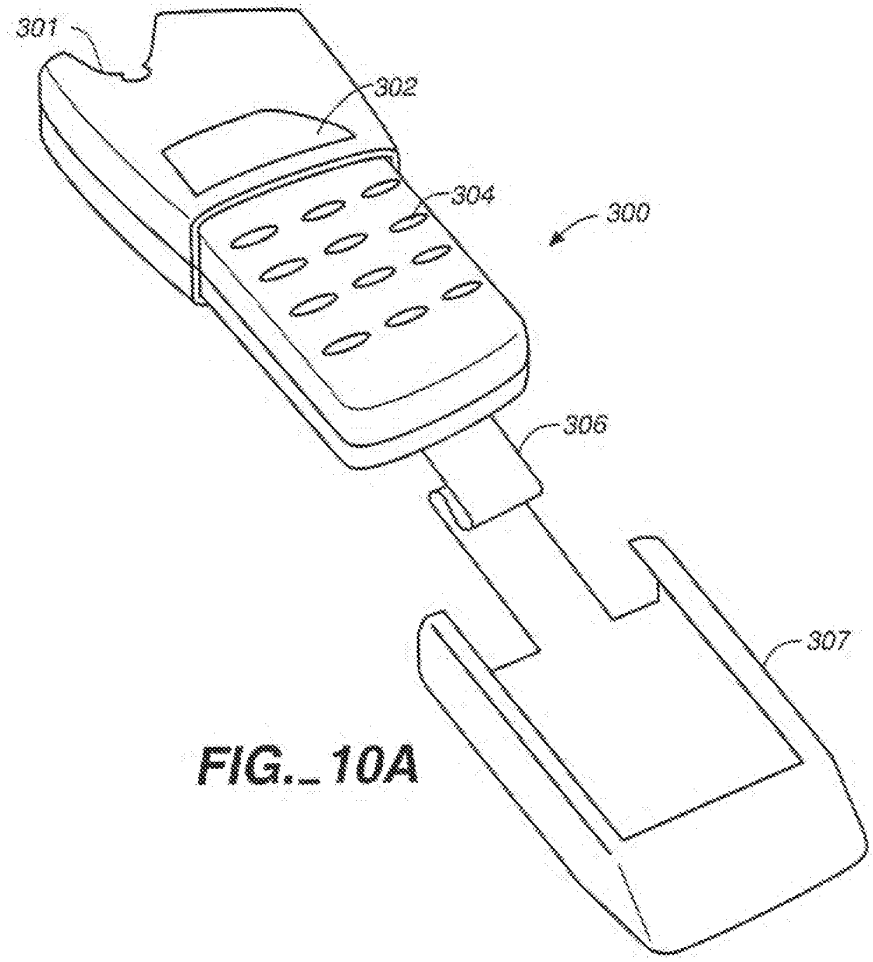


FIG._10A

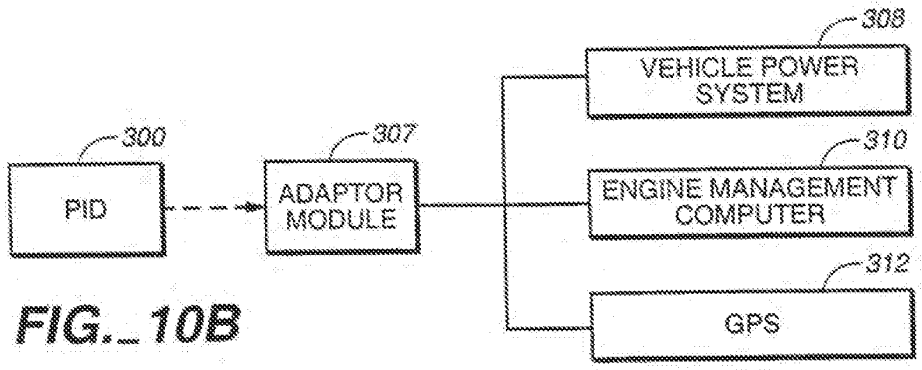


FIG._10B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/08990

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6): H04L 9/00; H04Q 1/00
US CL: 380/23; 382/115,116
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)
U.S. : 380/23; 382/115,116,125,126,127,313; 356/71; 340/825.34; 713/202

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 practicable, search terms used)
Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,623,552 A (LANE) 22 April 1997, col.2, lines 29-35, col.3, lines 28-35,54-55, col.6, lines 42-44	1-2,13-14,29, --- 3-9,30-36, 38,40-41, 43,45
Y,E	US 5,903,225 A (SCHMITT et al) 11 May 1999, col.2, lines 53-60, col.4, lines 63-65,66-67, col.13, lines 40-65	3-9,30-36, 38,40-41, 43,45
A	US 5,546,471 A (MERJANIAN) 13 August 1996, col.2, lines 39-46, col.6, lines 48-54, col.11, lines 25-31.	3,4-5,25
A	US 4,995,086 A (LILLEY et al) 19 February 1991, col.2, lines 10-18, col.3, lines 10-15, col.4, lines 62-68	1-2,13,21

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document 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
10 JUNE 1999	08JUL1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3040	Authorized officer GAIL HAYES Telephone No. (703) 305-0042

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/08990

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

APS
search terms: biometric, fingerprint, finger print, thumb print, thumbprint, password, ID code, key, transmit, send, portable, device, wireless, authentication

Form PCT/ISA/210 (extra sheet)(July 1992) *

Trials@uspto.gov
571-272-7822

Paper 12
Date: February 28, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2021-01447
Patent 9,298,905 B1

Before KEVIN F. TURNER, JUSTIN T. ARBES, and DAVID C. McKONE, *Administrative Patent Judges.*

TURNER, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background and Summary

Petitioner Samsung Electronics America, Inc. filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1–12 of U.S. Patent No. 9,298,905 B1 (Ex. 1001, "the '905 Patent") pursuant to 35 U.S.C. § 311(a). Patent Owner Proxense, LLC filed a Preliminary Response (Paper 10, "Prelim. Resp.") pursuant to 35 U.S.C. § 313.

Pursuant to 35 U.S.C. § 314(a), the Director may not authorize an *inter partes* review unless the information in the petition and preliminary response "shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." *See* 37 C.F.R. § 42.4(a) ("The Board institutes the trial on behalf of the Director."). For the reasons that follow, we do not institute an *inter partes* review.

B. Related Matters

The parties indicate that the '905 Patent is the subject of *Proxense, LLC v. Samsung Electronics Co., Ltd.*, Case No. 6:21-cv-00210 (W.D. Tex.) ("the district court case"). *See* Pet. 3; Paper 5, 1. Petitioner also filed petitions challenging claims of other patents asserted in the district court case: Cases IPR2021-01438, IPR2021-01439, IPR2021-01444, and IPR2021-01448.

C. The '905 Patent

The '905 Patent discloses systems for "authentication responsive to biometric verification of a user being authenticated," using "a persistent storage to persistently store[] a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format." Ex. 1001, 1:65–67.

The '905 Patent states that "[c]onventional user authentication techniques," such as requiring input of a password, were deficient because they "require[d] the user to memorize or otherwise keep track of the credentials" and "it can be quite difficult to keep track of them all." *Id.* at 1:28–37. Other techniques, such as "provid[ing] the user with an access object . . . that the user can present to obtain access," were inadequate because "authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object." *Id.* at 1:38–46. According to the '905 Patent, there was a need in the art for a system for "verifying a user that is being authenticated that does not suffer from [such] limitations" and "ease[s] authentications by wirelessly providing an identification of the user." *Id.* at 1:55–58.

Figure 2 of the '905 Patent is reproduced below.

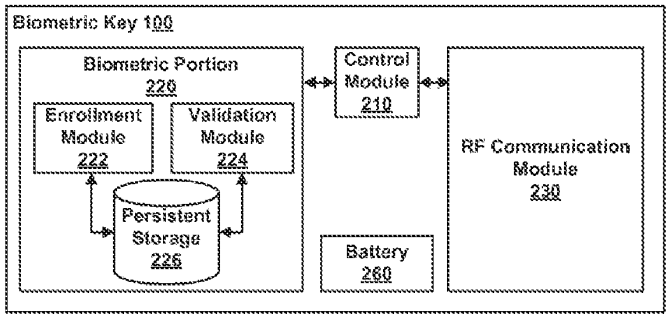


FIG. 2

Figure 2 is a block diagram of the functional modules of a biometric key. Ex. 1001, 3:30–33, 4:42–43. Enrollment module 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user (e.g., a digital image of the retina, fingerprint, or voice sample) in persistent storage 226. *Id.* at 4:67–5:23. Enrollment module 222 registers biometric key 100 with a trusted authority by providing a code, such as a device ID, to the trusted authority or, alternatively, the trusted authority can

provide a code to biometric key 100. *Id.* at 5:3–7. The code is stored in persistent storage 226. *Id.* at 5:24–26. "Persistent storage 226 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data." *Id.* at 5:31–33. "Tamper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data)." *Id.* at 5:33–36. In a fingerprint embodiment, validation module 224 uses scan pad 120 (shown in Figure 1) to capture scan data from the user's fingerprint and compares the scanned data to the stored fingerprint to determine whether the scanned data matches the stored data. *Id.* at 5:8–12.

The interaction of biometric key 100 with other system components is illustrated in Figure 3, reproduced below.

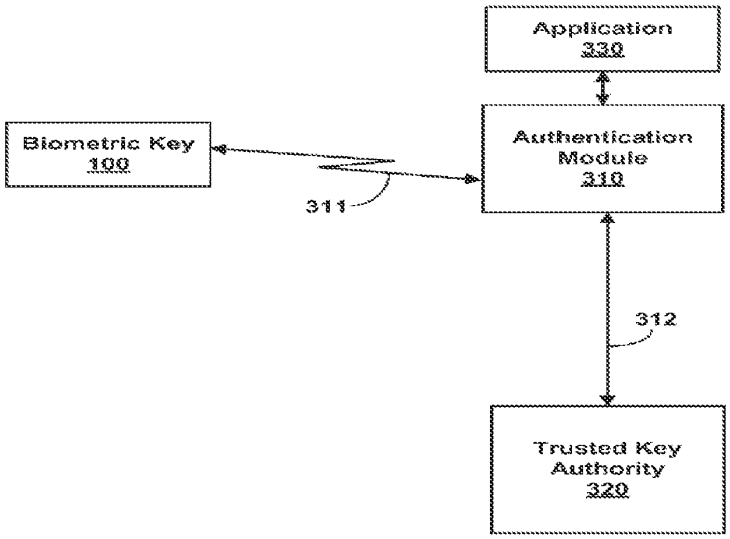


FIG. 3

Figure 3 is "a block diagram illustrating a system for providing authentication information for a biometrically verified user." Ex. 1001,

3:33–35. Authentication module 310 is coupled to biometric key 100 via line 311 (a wireless medium) and with trusted key authority 320 via line 312 (a secure data network such as the Internet). *Id.* at 5:67–6:7. Authentication module 310 requires the device ID code (indicating successful biometric verification) from biometric key 100 before allowing the user to access application 330. *Id.* at 6:10–13. Authentication module 310 provides the device ID code from biometric key 100 to trusted key authority 320 to verify that it belongs to a legitimate key. *Id.* at 6:13–19; *see also id.* 6:39–45 ("In one embodiment, trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the trusted key authority 320 stores a list of codes for legitimate biometric keys. . . . In one embodiment, trusted key authority 320 can also store a profile associated with a biometric key."). Authentication module 310 then sends a message to application 330 to allow the user access to the application responsive to a successful authentication by trusted key authority 320. *Id.* at 6:17–19.

"Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account . . . and the like." Ex. 1001, 6:21–26. Trusted key authority 320 can be operated by an agent, such as "a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." *Id.* at 7:33–36. "The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user." *Id.* at 7:36–39.

D. Illustrative Claim

Challenged claims 1 and 9 of the '905 Patent are independent. Claims 2–8 and 10–12 depend directly or indirectly from claim 1, although the language of certain claims suggests that the Patentee may have intended certain claims to have different dependencies. *See* Pet. 34 (taking no position regarding potential indefiniteness due to the dependencies). Claims 13–18 also issued with the '905 Patent, but are not challenged.

Claim 1 recites (with letter designations used in the Petition (Pet. iv) to refer to the various limitations):

> 1. A method comprising:
>
> [A] persistently storing biometric data of a legitimate user and an ID code on an integrated device;
>
> [B] responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;
>
> [C] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
>
> [D] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
>
> [E] responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction.

Ex. 1001, 10:11–28.

E. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability (Pet. 5), supported by the declaration of Dr. Andrew Wolfe (Ex. 1003) in support of its contentions:

Claim(s) Challenged	35 U.S.C. §	References/Basis
1, 3–10, 12	103(a)[1]	Scott[2], Lapsley[3]
2, 11	103(a)	Scott, Lapsley, Robinson[4]
1, 3–7, 9, 10, 12	103(a)	Berardi[5], Shreve[6], Kinoshita[7]

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. § 103. Because the challenged claims of the '905 Patent have an effective filing date before the effective date of the applicable AIA amendment, we refer to the pre-AIA version of 35 U.S.C. § 103. *See* Ex. 1001, codes (22), (60).

[2] International Patent Application Publication No. WO 99/56429, published Nov. 4, 1999 (Ex. 1005, "Scott"); when referencing portions of Scott, we refer to the original publication's page numbers in the top-center of each page (not the page numbers added by Petitioner in the lower-right corner of each page), consistent with the parties' usage in their papers.

[3] US Patent Application Publication No. 2001/0000535 A1, published Apr. 26, 2001 (Ex. 1007, "Lapsley").

[4] US Patent Application Publication No. 2003/0177102 A1, published Sept. 18, 2003 (Ex. 1008, "Robinson").

[5] US Patent No. 7,239,226 B2, filed July 9, 2002, issued July 3, 2007 (Ex. 1010, "Berardi").

[6] US Patent Application Publication No. 2002/0109580 A1, published Aug. 15, 2002 (Ex. 1012, "Shreve").

[7] US Patent Application Publication No. 2003/0055792 A1, published Mar. 20, 2003 (Ex. 1013, "Kinoshita").

II. ANALYSIS

A. Discretionary Denial Under 35 U.S.C. § 314(a)

Institution of *inter partes* review is discretionary. *See Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) ("[T]he PTO is permitted, but never compelled, to institute an [*inter partes* review (IPR)] proceeding."); 35 U.S.C. § 314(a) ("The Director *may not* authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." (emphasis added)). In the Preliminary Response, Patent Owner argues that we should exercise our discretion to deny the Petition in view of the district court case, where Petitioner previously asserted that we should not exercise our discretion to deny institution. Prelim. Resp. 4–6; Pet. 13–19. We need not decide this issue, however, as we determine that Petitioner has not shown a reasonable likelihood that it would prevail with respect to at least one of the challenged claims.

B. Legal Standards

A claim is unpatentable for obviousness if, to one of ordinary skill in the pertinent art, "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103(a) (2006)). The question of obviousness is resolved on the basis of underlying factual determinations, including "the scope and content of the prior art"; "differences between the prior art and the claims at issue"; and "the level of

ordinary skill in the pertinent art." *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Additionally, secondary considerations, such as "commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy." *Id.* When conducting an obviousness analysis, we consider a prior art reference "not only for what it expressly teaches, but also for what it fairly suggests." *Bradium Techs. LLC v. Iancu*, 923 F.3d 1032, 1049 (Fed. Cir. 2019) (citation omitted).

A patent claim "is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418. An obviousness determination requires finding "both 'that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.'" *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016) (citation omitted); *see KSR*, 550 U.S. at 418 (for an obviousness analysis, "it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does").

"Although the *KSR* test is flexible, the Board 'must still be careful not to allow hindsight reconstruction of references . . . without any explanation as to *how* or *why* the references would be combined to produce the claimed invention.'" *TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1066 (Fed. Cir. 2016) (citation omitted). Further, an assertion of obviousness "cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal

conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); *accord In re NuVasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (stating that "conclusory statements" amount to an "insufficient articulation[] of motivation to combine"; "instead, the finding must be supported by a 'reasoned explanation'" (citation omitted)); *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) ("To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.").

C. Level of Ordinary Skill in the Art

Petitioner argues that at the time of the '905 Patent, a person of ordinary skill in the art would have had "a bachelor's degree in computer or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent)." Pet. 4. Patent Owner does not address the level of ordinary skill in the art in its Preliminary Response. Based on the record presented, including our review of the '905 Patent and the types of problems and solutions described in the '905 Patent and cited prior art, we adopt Petitioner's definition of the level of ordinary skill in the art and apply it for purposes of this Decision.

D. Claim Interpretation

We interpret the challenged claims

> using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

37 C.F.R. § 42.100(b) (2021). "In determining the meaning of [a] disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006). Claim terms are generally given their ordinary and customary meaning as would be understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). "There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

Petitioner submits that no express interpretations of any claim terms are necessary to resolve the parties' dispute and "the claim terms should be given their plain and ordinary meaning." Pet. 7. Patent Owner identifies two claim terms, "third-party trusted authority" and "access message," both recited in independent claims 1 and 9, that it presents as being edifying, based on Petitioner's Opening Claim Construction Brief in the district court case (Ex. 2001), and its own Responsive Claim Construction Brief (Ex. 2002). Prelim. Resp. 2–4.

Patent Owner points out that Petitioner argued in the district court case that a "third-party" is "an entity with a responsibility separate from executing the transaction itself." Prelim. Resp. 2 (quoting Ex. 2001, 7). In the district court case, Petitioner argued that no construction of "third-party trusted authority" was needed and "[t]he intrinsic evidence does not suggest

a party or component numbered after a second party." Ex. 2001, 6–7. This was in response to its articulation of Patent Owner's position, namely, that a "third-party trusted authority" is "[a] third component that provides a second level of authentication." *Id.* at 6.[8]

Petitioner further argued that "[d]uring prosecution, the applicant explained a 'user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation," and "[t]he applicant emphasized the prior art 'disclose[d] two parties: the user and the institution.'" Ex. 2001, 7 (quoting remarks made by the applicant for a related patent accompanying an amendment and addressing the same claim term) (alterations by Petitioner). Petitioner argued that "the intrinsic evidence suggests 'third party' relates to a specific class of entity occupying the aforementioned particular relationship." *Id.* Petitioner then pointed out that "the [S]pecification [of the related patent] explains the agent for the trusted authority 'can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness.'" *Id.* According to Petitioner, "[t]his 'witness' role further aligns with prosecution history where the applicant explained 'sending a code to a receiver of a *door that the user is trying to access*' does not satisfy the 'third party' limitation." *Id.* (quoting an amendment in the related patent file history).

[8] In its responsive brief, Patent Owner changed its position with respect to the terms "third-party trusted authority" and "agent" to "[n]o construction needed" and stated that it "no longer seeks to submit th[e] term[s] for construction." Ex. 2002, 12. The district court did not construe the terms. Ex. 3001.

Petitioner further offered expert testimony in the district court case to support an argument that "[c]ommon industry use of 'trusted third party' identifies 'third party' as an entity with a responsibility separate from executing the transaction itself." *Id.* at 7–8 (citing a declaration of Seth James Nielson, Ph.D. (Ex. 2003 ¶¶ 70–74) and a book, CRYPTOGRAPHIC LIBRARIES FOR DEVELOPERS). Dr. Nielson appears to best articulate the distinction Petitioner was drawing between a third component and a third entity: "the [S]pecification, the prosecution history, and common industry usage all suggest a 'third party' refers to an entity outside of the transaction or a witness thereto rather than a 'third component.'" Ex. 2003 ¶ 74.

In light of Petitioner's arguments in the district court case, Patent Owner contends that the parties "agree that a 'third-party trusted authority' is an institution or entity that is outside of the multi-party system (user and application or vendor) that is being authenticated." Prelim. Resp. 3.

We agree with Patent Owner. The plain meaning of "third-party trusted authority" suggests an entity or party separate from the principal parties to a transaction. *See, e.g.*, THE AMERICAN HERITAGE COLLEGE DICTIONARY 1433 (4th ed. 2004) ("third party n. . . . 2. One other than the principals involved in a transaction.") (Ex. 3002).

This is consistent with the description in the Specification. For example, Figure 3, reproduced above, depicts trusted key authority 320 as an entity separate from biometric key 100, authentication module 310, and application 330. As the Specification states, "[t]rusted key authority 320 is a third-party authority that is present in some embodiments in order to provide enhanced security." Ex. 1001, 6:37–39. Examples of trusted key authorities include "a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." *Id.* at

7:33–36. Petitioner's citations to the applicant's statement during prosecution of the related patent also are consistent with a third-party trusted authority being an entity separate from the principal parties to a transaction, as is the declaration of Dr. Nielson. *See* Ex. 2001, 6–8; Ex. 2003 ¶¶ 70–74. Thus, we interpret "third-party trusted authority" to mean a trusted authority that is an entity separate from the parties to a transaction.

Claim 1 also recites "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code," with claim 9 providing a similar recitation. Patent Owner argues that "[a]n 'access message' must be sent by the 'third party trusted authority'" and the parties "agree that the 'access message' originates from the 'third-party trusted authority' and communicates information regarding authentication." Prelim. Resp. 3–4 (citing Ex. 2001, 9). Given the express requirement in claims 1 and 9 that the access message be received "from" the third-party trusted authority, we conclude that no further interpretation of the "access message" limitations is necessary.[9]

E. Obviousness Ground Based on Scott and Lapsley

Petitioner contends that claims 1, 3–10, and 12 are unpatentable over Scott and Lapsley under 35 U.S.C. § 103(a). Pet. 19–34. Patent Owner argues that the Petition fails to demonstrate that the combination of references teaches or suggests all elements of the challenged claims. Prelim.

[9] Petitioner argued in the district court case that the limitations mean "[r]eceiving a signal from the agent permitting a user to access an application," Patent Owner argued that no construction was necessary and the phrases should be given their plain and ordinary meaning, and the district court determined that no construction was necessary. Ex. 3001, 3.

Resp. 6–9. We are not persuaded that Petitioner has established a reasonable likelihood of prevailing on this asserted ground as to any of the challenged claims. We begin with short discussions of Scott and Lapsley, and discuss Petitioner's contentions and Patent Owner's arguments thereafter.

1. Scott

Scott describes "a portable personal identification device for providing secure access to a host facility" in which the device "includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and provid[es] a biometric signal indicative thereof." Ex. 1005, 2:5–8. Figure 1 of Scott, reproduced below, illustrates an example.

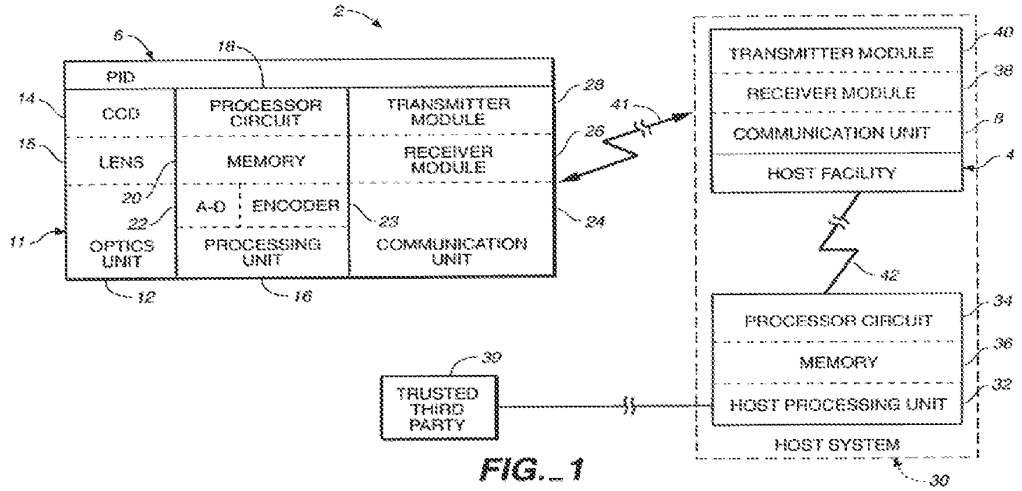


FIG._1

Figure 1 is a block diagram of security system 2 that provides access to host facility 4 (e.g., a bank, store, military base, computer system, automobile, home security system, or gate). *Id.* at 10:l, 24–28.

A registered person carries battery powered personal identification device (PID) 6 (e.g., similar in size to a hand-held pager), which includes biometric sensor 11. *Id.* at 10:28–11:5. Memory 20 stores an ID code that is set in PID 6 by the manufacturer. *Id.* at 11:11–13. The owner of PID 6

enrolls into the unit by scanning a finger using biometric sensor 11 to create an image that is stored as the fingerprint template in memory 20. *Id.* at 11:14–20, 15:30–16:6. PID 6 communicates wirelessly via transmission signal 41 with host facility 4. *Id.* at 12:14–16.

Host facility 4 is part of host system 30 (e.g., a bank ATM system or point of sale system), which also includes host processing unit 32. *Id.* at 11:31–12:2. "Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42." *Id.* at 12:3–5. "Memory 36 stores ID codes of enrolled individuals who have registered with host system 30." *Id.* at 12:6–7.

Figure 7 of Scott is reproduced below.

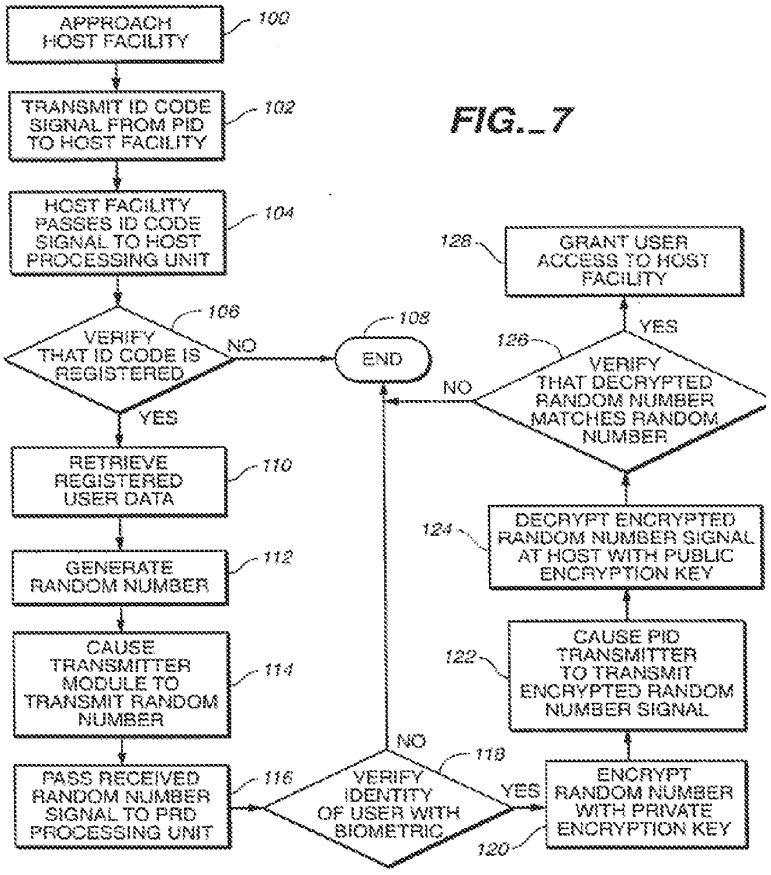


FIG._7

Figure 7 is a flow diagram of a method of accessing a host facility with a personal identification device. *Id.* at 10:13–14.

A user with PID 6 approaches host facility 4 (e.g., an ATM) and transmits the ID code to host receiver module 38, which passes it to host processing unit 32. *Id.* at 17:20–27 (steps 100–104). Host processing unit 32 verifies that the received ID code represents a registered ID code and, if so, the account or user information is located. *Id.* at 17:27–30 (steps 106, 110). Host processing unit 32, via transmitter module 40, sends a random number to PID 6, in response to which PID 6 performs a user verification. *Id.* at 18:1–4 (steps 112–118). PID 6 verifies the user's fingerprint when the user places their finger on platen 15 of biometric sensor 11 by comparing the

fingerprint signal to the stored fingerprint template. *Id.* at 16:19–29. If PID 6 successfully verifies the user's fingerprint, PID 6 encrypts the random number and sends it back to host processing unit 32, which decrypts the random number and verifies that it matches the random number it sent to PID 6. *Id.* at 18:5–14 (steps 120–126). If the random number is a match, host processing unit 32 grants the user access to host facility 4. *Id.* at 18:14–15 (step 128).

2. Lapsley

Lapsley describes "a system and method of using biometrics for processing electronic financial transactions such as on-line debit, off-line debit and credit transactions without requiring the user to directly use or possess any man-made tokens such as debit or credit cards or checks." Ex. 1007 ¶ 2.

Figure 2 of Lapsley, reproduced below, illustrates an example.

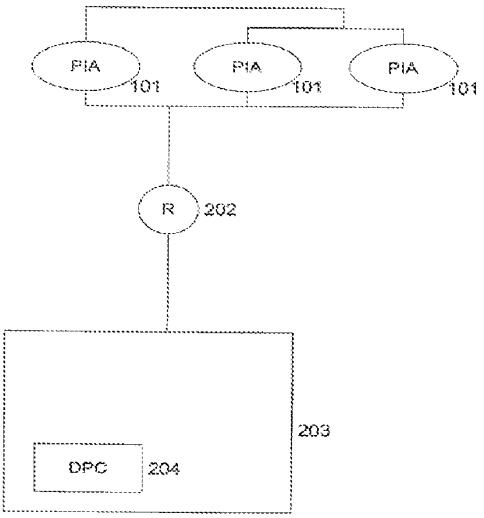


Figure 2 is a block diagram showing the connections among Party Identification Devices (PIAs) 101, router 202, and Network Operations Center (NOC) 203. *Id.* ¶ 47. Figure 2 is in the context of a supermarket

chain or other multi-lane retail chain with multiple PIAs 101 connected via an in-store local area network to local router 202, which is connected to NOC 203 via frame relay lines. *Id.* ¶ 98. NOC 203 includes Data Processing Center (DPC) 204. *Id.*

Each PIA 101 has a hardware identification code that is assigned to it and registered with DPC 204 at the time of manufacture, making the PIA uniquely identifiable to DPC 204 in transmissions from the PIA. *Id.* ¶¶ 85, 161. An entity uses the PIA hardware identification code to identify itself to the DPC. *Id.* ¶ 158.

Figure 7 of Lapsley is reproduced below.

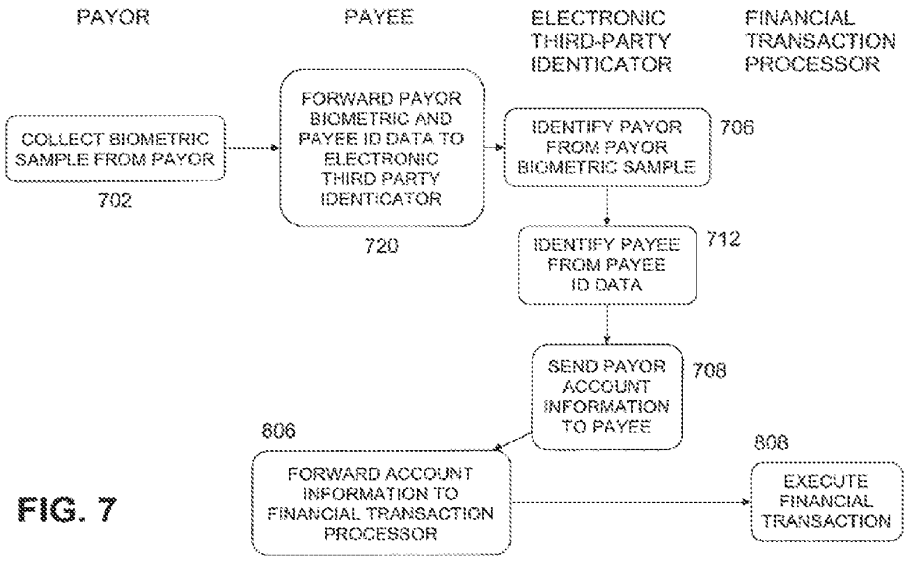


FIG. 7

Figure 7 is a flow diagram showing a transaction flow among the participants in a retail point-of-sale transaction. *Id.* ¶¶ 52, 166.

The customer/payor originates an electronic payment at a point-of-sale by submitting a bid biometric sample obtained by a biometric sensor of the PIA controlled by a payee/seller. *Id.* ¶¶ 166–167 (step 702). The PIA determines that the sample is not fraudulent and sends the sample to the DPC. *Id.* ¶ 167. The payor enters a PIN code into the PIA, and the

PIA transmits the biometric data, PIN, and hardware identification code of the PIA to the DPC. *Id.* ¶ 168 (step 720). The DPC identifies the payor using the biometric sample, retrieves a list of financial accounts that the payor has registered with the system, and transmits the list to the PIA. *Id.* (steps 706, 708). The DPC identifies the payee using the PIA hardware identification code. *Id.* ¶¶ 166, 168. The payor selects a financial account at the PIA, and the PIA transmits the financial information to the payee's in-store payment system (e.g., point-of-sale terminal or electronic cash register). *Id.* ¶¶ 169–170. The in-store payment system authorizes the transaction. *Id.* ¶ 170.

3. Claim 1

Petitioner argues that Scott and Lapsley collectively teach all of the limitations of claim 1. Pet. 19–26. With respect to the preamble of claim 1, Petitioner contends that Scott teaches a method of verifying a user during authentication of an integrated device (i.e., PID 6). *Id.* at 19.

With respect to limitation A, Petitioner argues that Scott teaches persistently storing "biometric data of a user" in memory 20 of PID 6 and persistently storing a plurality of codes and other data values including an ID code that uniquely identifies PID 6, where the ID code may be set by the device manufacturer and can be the device serial number. Pet. 20–21 (citing Ex. 1005 4:1–18, 6:28–7:23, 8:13–22, 11:11–20, 13:10–15, 15:30–16:6, 19:30–32).

With respect to limitation B, Petitioner argues that Scott discloses receiving a request for a biometric verification of the user by pressing a "verify" button on PID 6, and in response to this request, PID 6 can receive scan data from a biometric scan, such as a fingerprint scan from the user

placing a finger on platen 15, a voice biometric scan, "or any other type of biometric scan." Pet. 21–22 (citing Ex. 1005, 3:21–32, 16:19–29, Fig. 4A).

With respect to limitation C, Petitioner argues that Scott discloses that after receiving the biometric scan data, PID 6 compares the received biometric scan data (e.g., voice, iris, or fingerprint biometric) to a stored biometric template in order to verify the user's identity. Pet. 22 (citing Ex. 1005, 15:30–16:29).

With respect to the first portion of limitation D, Petitioner relies on the teachings of Scott. Pet. 22–23. As to the limitation of "responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code," Petitioner contends that, in response to the comparison discussed in connection with limitations B and C above, Scott's PID 6 wirelessly transmits to host facility 4 "an encrypted message with [the] ID code and other data such as a synchronization counter." *Id.* (citing Ex. 1005, 4:6–18, 5:22–6:24, 6:28–7:23).

With respect to the second portion of limitation D, namely "for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," Petitioner contends that "Scott discloses that the third-party trusted authority host processing unit 32 stores a list that includes an ID code and a public key for each registered PID 6," and host processing unit 32 compares the device ID code received from PID 6 to this list to authenticate PID 6 as a legitimately registered device. *Id.* at 23–24 (citing 5:10–21, 6:11–21, 7:24–8:4, 8:18–22; 9:23–25, 11:12–13, 12:6–13, 13:10–15, 19:18–20, 30–32, Fig. 1). Although not cited in the Petition, Dr. Wolfe repeats these arguments in his testimony. *See* Ex. 1003 ¶ 45. Petitioner and Dr. Wolfe thus identify Scott's host processing unit 32 as corresponding to the claimed

"third-party trusted authority." Also, in its analysis of limitation E of claim 1, Petitioner makes clear that host facility 4 is the application (e.g., key card entry, ATM machine, garage door opener) that is accessed when the transaction is completed. Pet. 26 (citing Ex. 1005, 17:20–18:19, 5:10–21, 8:5–12).

Patent Owner argues that "host processing unit 32 is *part of* the system being accessed—it is not a third party." Prelim. Resp. 7 (citing Ex. 1005, 11:24–25, 11:30–12:1). As explained above, a "third-party trusted authority" is a trusted authority that is an entity separate from the parties to a transaction. *See supra* Section II.D. Scott describes both host processing unit 32 (the alleged "third-party trusted authority") and host facility 4 (the alleged application to be accessed by the user, "selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file") as part of a single entity, host system 30. Ex. 1005, 11:31–12:5 ("Host facility 4 is part of a host system 30. Host system 30 will typically be bank ATM systems, point of sale systems, and the like. Host system 30 also includes a host processing unit 32, which has a processor circuit 34 and memory 36 . . . . Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42."). As such, host processing unit 32, because it is not an entity separate from host facility 4, is not a third-party trusted authority.

Petitioner further argues that, "[t]o the extent [that Patent Owner] argues that Scott's host processing unit 32 is not a third-party trusted authority, Lapsley . . . provides additional disclosure rendering this feature of the limitation obvious to a [person of ordinary skill in the art]." Pet. 24.

Petitioner contends that Lapsley's DPC is a trusted third-party authority that receives biometric data and a hardware identification code from a PIA and uniquely identifies the PIA by finding the identification code on a list the DPC maintains. *Id.* at 24–25 (citing Ex. 1007 ¶¶ 54, 82, 85, 103, 104, 158, 161, 166–168).

Relying on Dr. Wolfe's testimony, Petitioner argues that a person of ordinary skill in the art

> would have been motivated to modify Scott's system such that authentication is performed by an external third-party trusted authority possessing a list of device ID codes that unique[ly] identify legitimate PIDs, as taught in Lapsley, to improve efficiency and flexibility of the system by consolidating ID codes to a central location at a secure third-party agent.

Pet. 25 (citing Ex. 1003 ¶ 47). Dr. Wolfe repeats this argument in his testimony, but does not state the basis for his opinion, rendering it of little value. *See* 37 C.F.R. § 42.65(a). Citing to Lapsley, Petitioner argues that an ordinarily skilled artisan "would have recognized the benefit in reducing the risk of fraud by improving security and authentication by using a trusted third-party agent to verify devices involved in a transaction." *Id.* (citing Ex. 1007 ¶¶ 8, 9, 27, 29). Petitioner argues that an ordinarily skilled artisan "would have further understood that it was common to have an ATM that is not owned by a bank use the bank as a third party for authorization and it was common for a store to use a bank or credit card exchange as a third party for authorization." *Id.* at 26. Petitioner does not cite any evidence for this argument.

Patent Owner responds that "Lapsley's DPC is part of the system providing access to a user's registered financial accounts, *i.e.*, a cloud based digital wallet—not a *third party* trusted authority." Prelim. Resp. 8 (citing

Ex. 1007 ¶¶ 102, 138, 139). Patent Owner contends that, "[i]n Lapsley, instead of using a personal fob or phone to access the DPC digital wallet, the user utilizes a Party Identification Apparatus located at a store." *Id.* at 8–9 (citing Ex. 1007 ¶¶ 167–169). According to Patent Owner, "[a]s the DPC is accessed with the PIA to retrieve a list of user financial accounts stored in the DPC, the DPC must be the system being accessed/authenticated. Consequently, Lapsley's DPC is not what the Petitioner and Patent Owner agree constitutes a 'third-party trusted authority.'" *Id.* at 9.

We agree with Patent Owner. Petitioner has not explained sufficiently why Lapsley's DPC is a third-party trusted authority, what entities the DPC is a third-party relative to, or what application the user is being permitted to access in the asserted combination. As Patent Owner points out, the DPC appears to be what is being accessed, as the payee and payor, with the PIA, access a list of financial accounts from the DPC. *See id.* at 8–9; Ex. 1007 ¶¶ 167–170. Here, the DPC is the resource to be accessed, but it is a party to the transaction, rather than a third party. This is similar to the situation Petitioner argues that the applicant distinguished during prosecution: "[d]uring prosecution, the applicant explained a 'user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation." *See* Ex. 2001, 7 (quoting remarks made by the applicant during prosecution of the related patent (alterations by Petitioner)).

Petitioner's reasons to combine also are conclusory and unsupported by persuasive evidence. In particular, Dr. Wolfe merely repeats Petitioner's arguments in his testimony, without further explaining them or identifying

the basis for his opinions.[10] *See* Ex. 1003 ¶ 48. We agree with Patent Owner that Petitioner has not shown that Lapsley teaches a "third-party trusted authority" or that a skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Scott and Lapsley.

Because Petitioner does not show persuasively that either Scott or Lapsley teaches a "third-party trusted authority," as recited in claim 1, or that an ordinarily skilled artisan would have combined the teachings of those references, Petitioner has not shown sufficiently that Scott and Lapsley teach limitation D:

> responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority.

Petitioner's ground fails for an additional reason as well. The claim plainly requires that the access message be received "from the third-party trusted authority," per limitation E.

Petitioner argues that "in response to authentication of the received ID code by comparing it to a stored ID code, the receiver module 26 of PID 6 receives a random number signal from [host processing unit 32] that enables access to a secure resource." Pet. 26 (citing Ex. 1005, 5:10–21, 8:5–12, 17:20–18:19). Petitioner does not provide any further explanation as to why Scott's host processing unit 32 allegedly constitutes a "third-party trusted authority." *See id.* Nor does Petitioner mention Lapsley, or the combined teachings of Scott and Lapsley, in addressing limitation E of claim 1. *See id.* Because Petitioner has not shown sufficiently that host processing unit 32 is

[10] Moreover, as explained below, the entirety of Dr. Wolfe's testimony lacks credibility and is entitled to little or no weight. *See infra* Section II.G.

a "third-party trusted authority," Petitioner likewise has not established that Scott's random number signal is an "access message [sent] from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code," as recited in limitation E of claim 1. *See* Prelim. Resp. 9.

Therefore, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claim 1 is unpatentable over Scott and Lapsley.

4. Claims 3–10 and 12

Independent claim 9 recites the same elements of independent claim 1, discussed above, that we determine that Petitioner's Petition has not shown according to this ground of unpatentability. *See* Ex. 1001, 10:54–11:3. Claims 3–8 and 10–12 ultimately depend from claim 1. For the reasons explained above regarding claim 1, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claims 3–10 and 12 are unpatentable over Scott and Lapsley.

F. Obviousness Ground Based on Scott, Lapsley, and Robinson

Petitioner contends that claims 2 and 11 are unpatentable over Scott, Lapsley, and Robinson under 35 U.S.C. § 103(a). Pet. 34–36. Claims 2 and 11 ultimately depend from claim 1. Petitioner does not argue that the additional reference (Robinson) teaches the missing limitations of parent claim 1, as discussed above. *See id.* Accordingly, for the reasons explained above, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claims 2 and 11 are unpatentable.

G. Obviousness Ground Based on Berardi, Shreve, and Kinoshita

Petitioner contends that claims 1, 3–7, 9, 10, 12 are unpatentable over Berardi, Shreve, and Kinoshita under 35 U.S.C. § 103(a), citing the testimony of Dr. Wolfe as support. Pet. 36–46 (citing Ex. 1003).

Petitioner's allegations and citations to Berardi do not correspond to the disclosure of that reference. *See* Prelim. Resp. 10 ("With regard to Berardi, Petitioner references elements and paragraphs not contained within Berardi at all, *i.e.*, in error.").[11]

For example, in alleging that Berardi teaches "responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," as recited in limitation D of claim 1, Petitioner argues that "issuer system 1010 [that] includes an issuer account server (IAS) 1014 that processes fob identifying information," of Berardi, corresponds to the claimed "third-party trusted authority." Pet. 38–39 (citing Ex. 1010, 10:56–11:12, 22:1–41, 28:50–67). Berardi does not describe an "issuer system 1010" or "issuer account server (IAS) 1014." The cited material in columns 10 and 11 is inapposite (and does not discuss issuer system 1010 or IAS 1014), Berardi ends its disclosure at line 30 (not line 41) of column 22, and column 28 does not exist in Berardi. Additionally, following the normal

[11] Patent Owner notes that Petitioner's errors "make[] it difficult to ascertain Petitioner's argument[s]," but argues that "a full reading of Berardi makes clear that it fails to disclose a 'third-party trusted authority.'" Prelim. Resp. 10. Patent Owner then presents substantive arguments as to Berardi, Shreve, and Kinoshita. *Id.* at 10–15. We deny the Petition as to this ground based on Petitioner's failure to present an understandable case as to Berardi and do not reach Patent Owner's additional arguments.

numbering of elements in patent drawings, the highest number referenced in Berardi is "906," short of the elements "1010" and "1014," discussed by Petitioner.

Also in its analysis of limitation E of claim 1, Petitioner states that Berardi discloses that "in response to authentication of the received identifying information of the fob 102, the POS device 110 may send 'an optical and/or audible transaction status message' to the RFID reader 104 for communication directly with the customer." Pet. 40–41 (citing Ex. 1010, 20:51-62, Fig. 8). Column 20, lines 51–62 of Berardi encompass a portion of claim 1 of Berardi, and the cited section does not discuss POS Device 110. Figure 8 of Berardi provides a flow diagram of an exemplary payment/transaction process, but does not detail sending an optical and/or audible message, as Petitioner alleges. We conclude that Petitioner did not simply misidentify or mislabel the components of Berardi it sought to reference.

There are numerous similar errors. For example, Petitioner relies on column 28, lines 50–67, which does not exist in Berardi, for limitations A, B and D of claim 1. *See* Pet. 37–39. Petitioner's citation to column 12, lines 36–41 in its analysis of limitation B of claim 1 does not correspond to biometric information, or anything else we can discern to be relevant to these limitations. *See id.* at 38. Instead, it discusses RFID reader 104 authenticating fob 102. Ex. 1010, 12:36–41. We do not intend to list all such errors here. We decline to speculate as to what Petitioner might have intended to cite. The result of the errors in the Petition is that we are unable to understand Petitioner's allegations and Patent Owner cannot fairly be said to be on notice of Petitioner's challenge based on Berardi.

Petitioner contends that (1) to the extent Berardi fails to teach limitation D of claim 1, Shreve provides additional disclosure; and (2) to the extent Berardi fails to teach limitation E of claim 1, Kinoshita provides additional disclosure. Pet. 39–41. However, because Petitioner has not sufficiently explained its allegations as to Berardi, it is impossible to understand Petitioner's proposed combination with Shreve and Kinoshita. Moreover, as explained above, Petitioner's arguments regarding limitations A, B, D, and E of claim 1 are based largely on material that does not exist in Berardi. Thus, even if we were able to discern Petitioner's arguments for limitations A, B, D, and E of claim 1, Petitioner's cited evidence does not support its allegations for other elements of claim 1.

Petitioner's allegations for independent claim 9 largely track or refer back to its analysis of claim 1 and, thus, suffer from the same defects. *See* Pet. 44–46. Petitioner's allegations for dependent claims 3–7, 10, and 12 do not shed any additional light on what Petitioner might have intended for claim 1, and instead largely cite irrelevant or non-existent material in Berardi. *Id.* at 42–44, 46.[12]

[12] We also express concern with Dr. Wolfe's testimony. Paragraphs 71–97 of his declaration (Exhibit 1003) appear to be a near carbon copy of pages 36–46 of the Petition, and include the Petition's citations to obviously incorrect or non-existent material in Berardi. These circumstances suggest a lack of attention, as even a cursory review would have shown that his testimony regarding Berardi includes numerous references to irrelevant or non-existent material, rendering that testimony not useful. This is not an instance of one or even a few inadvertent errors that might go missed upon a diligent review. The entirety of Dr. Wolfe's testimony regarding Berardi is defective on its face. For these reasons, the entirety of Dr. Wolfe's testimony lacks credibility and is entitled to little or no weight.

In sum, we cannot discern Petitioner's allegations of obviousness based on Berardi, Shreve, and Kinoshita, nor can we say Patent Owner is on notice of those allegations. Accordingly, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claims 1, 3–7, 9, 10, 12 are unpatentable over Berardi, Shreve, and Kinoshita.

III. CONCLUSION

Based on the arguments presented in the Petition, we conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to at least one claim of the '905 Patent challenged in the Petition. Therefore, we do not institute an *inter partes* review.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is denied and no *inter partes* review is instituted.

FOR PETITIONER:

James M. Glass
Marissa Ducca
Richard Lowry
Sean Gloth
QUINN EMANUEL URQUHART & SULLIVAN, LLP
jimglass@quinnemanuel.com
marissaducca@quinnemanuel.com
richardlowry@quinnemanuel.com
seangloth@quinnemanuel.com

FOR PATENT OWNER:

David L. Hecht
James Zak
HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

WACO DIVISION

PROXENSE, LLC, *Plaintiff*	§	
-v-	§	
	§	**6:21-CV-00210-ADA**
SAMSUNG ELECTRONICS CO., LTD. AND SAMSUNG ELECTRONICS AMERICA, INC., *Defendant*	§	JURY TRIAL DEMANDED

ORDER

Before the Court are the parties' claim construction briefs. Plaintiff Proxense, LLC (hereinafter "Proxense") submitted its Complaint *for Patent Infringement and Demand for Jury Trial* on April 23, 2021 (ECF No. 1). Defendants Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively "Samsung") submitted the opening *Markman* Brief on October 28, 2021, and the Reply Markman Brief on December 6, 2021. (ECF Nos. 33, 37, respectively). Plaintiff submitted its response on November 17, 2021, and sur-reply brief (ECF Nos. 35, 39, respectively). The Court held the *Markman* hearing on December 27, 2021. (ECF No. 42). This Order informs the parties of the Court's constructions.

I. Standard of Review

Generally, courts construe claim terms according to their plain and ordinary meaning. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*). The Federal Circuit applies a "heavy presumption" in favor of construing terms according to their plain and ordinary meaning, that is, the "meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Azure Networks, LLC v. CSR PLC*, 771 F.3d 1336, 1347 (Fed. Cir.

2014) (vacated on other grounds); *Phillips*, 415 F.3d at 1313. The "only two exceptions to [the] general rule" that claim terms are construed according to their plain and ordinary meaning are when the patentee acts as his own lexicographer or disavows the full scope of the claim term either in the specification or during prosecution. *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012). To act as his own lexicographer, the patentee must "clearly set forth a definition of the disputed claim term," and "clearly express an intent to define the term." *Id.* at 1365. To disavow the full scope of a claim term, the patentee's statements in the specification or prosecution history must represent "a clear disavowal of claim scope." *Id.* at 1366. Accordingly, when "an applicant's statements are amenable to multiple reasonable interpretations, they cannot be deemed clear and unmistakable." *3M Innovative Props. Co. v. Tredegar Corp.*, 725 F.3d 1315, 1326 (Fed. Cir. 2013).

While the specification "may aid the court" in analyzing disputed language in a claim, "particular embodiments and examples appearing in the specification will not generally be read into the claims." *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (internal citations omitted). Absent a "clear indication in the intrinsic record that the patentee intended the claims to be…limited," courts do not read limitations found in the specification into the claims. *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004).

II. Discussion

NO.	Claim Term	Plaintiff's Proposed Construction	Defendant's Proposed Construction	Court's Final Construction
1	**Persistently storing . . . a tamper proof format written to a storage element on the integrated device**	No construction necessary or possible, plain and ordinary meaning	Permanently storing in a form that prevents subsequent writing to store new data or	No construction necessary or possible, plain and ordinary meaning

	that is unable to be subsequently altered" (730:1, 15) / "a tamper proof format written to the memory that is unable to be subsequently altered" (730:8).		modifications to existing data	
2	**"device ID code" (730:1, 3, 8, 10, 12, 15) / "ID Code" (905:1-3, 8-11, 13-14; 989:1-2, 4-8)**	A unique code identifying a device	The device-specific code that identifies the device	A unique code identifying a device
3	**"receiving an access message from the agent allowing the user access to an application" (Claims 1, 8, 15) / "receiving an access message from the agent" (Claim 12)**	No construction necessary or possible, plain and ordinary meaning.	Receiving a signal from the agent permitting a user to access an application, / Receiving a signal from the agent permitting a user to access.	No construction necessary
4	**"access message" (Claims 1, 8, 12, 15)**	A signal or notification enabling or announcing access	A signal permitting a user to access.	A signal or notification enabling or announcing access
5	**"wherein the biometric data and the scan data are both based on a fingerprint scan by the user" (Claim 5).**	No construction needed, plain and ordinary meaning.	Invalid under §112 ¶4	No construction needed, plain and ordinary meaning.
6	**"hybrid device" (Claims 1-12,15, 20).**	A device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit.	Indefinite	A device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit.
7	**"Personal digital key" (Claims 1, 10).**	An operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for	A device that includes an antenna, a transceiver for communicating with the RDC and a controller and memory for storing	An operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for

		storing information particular to a user.	information particular to a user.	storing information particular to a user
8	**"biometric information" (Claims 1, 4, 10, 13).**	No construction necessary, plain and ordinary meaning.	The fingerprint, palm print, retinal scan, iris scan, photograph, signature, voice sample, or DNA/RNA information that uniquely identifies an individual.	No construction necessary, plain and ordinary meaning.
9	**"financial information" (Claims 5, 6, 14, 17).**	No construction necessary, plain and ordinary meaning. Alternatively, information about the transaction utilized to verify, authorize, or complete a transaction.	Purchasing account numbers, such as the debit card, ATM card, or bank account numbers.	No construction necessary, plain and ordinary meaning.
10	**"receiver-decoder circuit" (Claims 1, 10).**	A component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.	A device that provides a wireless interface to the PDK.	A component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.
11	**"inheritance information" (Claims 9, 18 (not asserted)).**	Information passed from a first device to a second device for use by the second device.	Information that is received from a predecessor device.	Information passed from a first device to a second device for use by the second device.
12	**"enablement signal" (Claims 10-12, 17)**	A message that enables or authorizes	No construction needed.	No construction needed.

			Alternatively, a signal that authorizes.	

SIGNED this 18th day of January, 2022.

SP 800-32

Introduction to Public Key Technology and the Federal PKI Infrastructure

D. Richard Kuhn
Vincent C. Hu
W. Timothy Polk
Shu-Jen Chang

26 February 2001

National Institute of Standards and Technology

National Institute of Standards and Technology, 2001. U.S. Government publication. Not subject to copyright.

Portions of this document have been abstracted from other U.S. Government publications, including: "Minimum Interoperability Specification for PKI Components (MISPC), Version 1" NIST SP 800-15, January 1998; "Certification Authority Systems", OCC 99-20, Office of the Comptroller of the Currency, May 4, 1999; "Guideline for Implementing Cryptography in the Federal Government", NIST SP800-21, November 1999; Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology, U.S. General Accounting Office, GAO-01-277, February, 2001.
Additional portions were used with permission from "Planning for PKI: Best practices for PKI Deployment", R. Housley and T. Polk, Wiley & Sons, 2001. John Wack contributed material on PKI architectures.

1 INTRODUCTION 5
1.1 GOALS 5
1.2 MOTIVATION 5
1.3 OVERVIEW 6
2 BACKGROUND 7
2.1 SECURITY SERVICES 7
2.2 NON-CRYPTOGRAPHIC SECURITY MECHANISMS 7
2.2.1 *Parity Bits and Cyclic Redundancy Checks* 7
2.2.2 *Digitized Signatures* 8
2.2.3 *PINs and Passwords* 8
2.2.4 *Biometrics* 8
2.2.5 *Summary - Non-Cryptographic Security Mechanisms* 9
2.3 CRYPTOGRAPHIC SECURITY MECHANISMS 9
2.3.1 *Symmetric Key* 9
2.3.2 *Secure Hash* 10
2.3.3 *Asymmetric (public key) Cryptography* 11
2.3.4 *Summary – Cryptographic Mechanisms* 12
2.4 SECURITY INFRASTRUCTURES 13
3 PUBLIC KEY INFRASTRUCTURES 15
3.1 PKI COMPONENTS 16
3.1.1 *Certification Authorities* 17
3.1.2 *Registration Authorities* 17
3.1.3 *PKI Repositories* 18
3.1.4 *Archives* 18
3.1.5 *PKI users* 18
3.2 PKI ARCHITECTURES 18
3.2.1 *Enterprise PKI Architectures* 19
3.2.2 *Bridge PKI Architecture* 20
3.2.3 *Physical Architecture* 20
3.3 PKI DATA STRUCTURES 22
3.3.1 *X.509 Public Key Certificates* 22
3.3.2 *Certificate Revocation Lists (CRLs)* 24
3.3.3 *Attribute Certificates* 26
3.4 ADDITIONAL PKI SERVICES 26
3.5 CASE STUDY 27
4 ISSUES AND RISKS IN CA SYSTEM OPERATION 29
4.1 VERIFYING IDENTITY 29
4.2 CERTIFICATE CONTENT 29
4.3 CERTIFICATE CREATION, DISTRIBUTION, AND ACCEPTANCE 30
4.4 MANAGING DIGITAL CERTIFICATES 30
4.4.1 *Customer Disclosures* 30
4.4.2 *Subscriber Service and Support* 31
4.4.3 *Suspending and Revoking Certificates* 31
4.4.4 *Processing Relying Party Requests* 32
4.4.5 *Certificate Revocation* 32
5 THE FEDERAL PKI 33
5.1 FEDERAL PKI ARCHITECTURE 33
5.2 FEDERAL CERTIFICATE PROFILE(S) 35
5.3 FEDERAL CRL PROFILE(S) 37
6 DEPLOYING AN AGENCY PKI 38

6.1 Analyze data and Applications for Your Organization 38
6.2 Collect Sample Policies and Base Standards 39
6.3 Draft Certificate Policy(s) 39
6.3.1 Certificate Policies *40*
6.3.2 Computer Security Objects Registry *41*
6.3.3 Establishing Policy Mappings and Constraints *41*
6.3.4 Local certificate and CRL profile(s) *41*
6.4 Select PKI Product or Service Provider 42
6.5 Develop CPS (Certification Practice Statement) 42
6.6 Do a Pilot 43
6.7 Apply for Cross Certification with the FBCA 43

7 SUMMARY AND CONCLUSIONS 44

8 ACRONYMS AND ABBREVIATIONS 45

9 GLOSSARY 46

10 SELECTED BIBLIOGRAPHY 53

1 INTRODUCTION

Public Key Infrastructures (PKIs) can speed up and simplify delivery of products and services by providing electronic approaches to processes that historically have been paper based. These electronic solutions depend on data integrity and authenticity. Both can be accomplished by binding a unique digital signature to an individual and ensuring that the digital signature cannot be forged. The individual can then digitally sign data and the recipient can verify the originator of the data and that the data has not been modified without the originator's knowledge. In addition, the PKI can provide encryption capabilities to ensure privacy.

As with all aspects of information technology, introducing a PKI into an organization requires careful planning and a thorough understanding of its relationship to other automated systems. This document provides a brief overview of issues related to the emerging Federal public key infrastructure, and its implementation within government agencies. It also reviews the risks and benefits of various PKI components, and some of the tradeoffs that are possible in the implementation and operation of PKIs within the Federal government.

1.1 GOALS

This publication was developed to assist agency decision-makers in determining if a PKI is appropriate for their agency, and how PKI services can be deployed most effectively within a Federal agency. It is intended to provide an overview of PKI functions and their applications. Additional documentation will be required to fully analyze the costs and benefits of PKI systems for agency use, and to develop plans for their implementation. This document provides a starting point and references to more comprehensive publications.

1.2 MOTIVATION

Practically every organization is looking to the Internet to deliver services, sell products, and cut costs. Federal agencies are under additional pressure to deliver Internet-based services to satisfy legislative and regulatory requirements. Two of the laws that motivate federal agencies to offer services electronically are the Government Paperwork Elimination Act (GPEA) [NARA 00] and the Health Insurance Portability and Accountability Act (HIPAA) [HCFA 01].

The Government Paperwork Elimination Act requires Federal agencies to offer services electronically. GPEA requires Federal agencies, by October 21, 2003, to provide an option to submit information or perform transactions electronically and to maintain records electronically. The law specifically establishes the legal standing of electronic records and their related electronic signatures.

Agencies are required to use electronic authentication methods to verify the identity of the sender and the integrity of electronic content. GPEA defines electronic signature as any method of signing an electronic message that identifies and authenticates the person who is the source of the message and indicates their approval of the contents.

The Health Insurance Portability and Accountability Act was passed in 1996. One part of this legislation was designed to improve efficiency through the use of uniform electronic data exchange mechanisms for health information. To achieve this, HIPAA required electronic processing and transmission of administrative and financial health care information. To address privacy and security concerns, HIPAA also mandates security and privacy standards to protect this health information.

Neither GPEA nor HIPAA mandates the use of specific technologies. Instead, they establish requirements to deliver services or transmit information while protecting the privacy and integrity of the citizen. However, the broad range of requirements established in these laws promotes the use of a comprehensive security infrastructure, such as PKI. Digital signatures and PKI offer a very strong mechanism to implement these requirements.

1.3 Overview

This document is divided into six sections. This section describes the motivations and contents of the document. Section 2, Background, describes the security services, mechanisms that have been used historically, and the rationale for supporting these services through a public key infrastructure. This section also explains why traditional security mechanisms may need to be supplemented with PKI functions for many applications. Section 3, Public Key Infrastructures, describes the technology on which PKI is based, and shows how public key systems provide security. Section 4 is devoted to operation of a key PKI component, the certification authority. In this section, some of the risk/benefit tradeoffs in operating an agency PKI system are described. Section 5 introduces the Federal PKI (FPKI) and some of the considerations for agencies that plan to connect with the FPKI. Finally, Section 6 provides a brief overview of the procedures required to set up a PKI within a Federal agency.

2 BACKGROUND

This section is intended to describe the security services that may be achieved, and provide a comparison for the various techniques that may be used.

2.1 SECURITY SERVICES

There are four basic security services: integrity, confidentiality, identification and authentication, and non-repudiation. This section describes the four services and why they may be necessary in a particular application.

Data integrity services address the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect *unauthorized* data modification. The goal is for the receiver of the data to verify that the data has not been altered.

Confidentiality services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the *unauthorized* disclosure of information to unauthorized individuals or processes.

Identification and authentication services establish the validity of a transmission, message, and its originator. The goal is for the receiver of the data to determine its origin.

Non-repudiation services prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

2.2 NON-CRYPTOGRAPHIC SECURITY MECHANISMS

Some of the security services described above can be achieved without the use of cryptography. Where illustrations may be useful, we will use Alice, Bob, and Charlie. Alice and Bob want to communicate in a secure manner. Charlie would like to interfere with the security services that Alice and Bob would like to obtain.

2.2.1 Parity Bits and Cyclic Redundancy Checks

The simplest security mechanisms were designed to ensure the integrity of data transmitted between devices (e.g., computers and terminals). When devices communicate over a noisy channel, such as a phone line, there was a possibility that data might be altered. To guard against this, systems would transmit an extra bit, the parity bit, for each byte of data. The value of the extra bit was chosen to ensure that the number of 1s in the nine bits were odd (odd parity) or even (even parity). If the parity was wrong, data had been altered, and should be rejected. This mechanism is frequently used with modem connections.

Parity bits are a relatively expensive form of integrity protection. They increase the size of the message by at least 12.5%. Worse, they may not detect multiple errors in the same byte. While this mechanism can be extended to detect such errors by using additional parity bits, the cost is increased yet again.

Cyclic redundancy checks, or CRCs, perform the same function for larger streams of data with less overhead. CRCs are calculated by the sender using a mathematical function applied to the data to be transmitted to create a fixed size output. The CRC is appended to the transmitted data. The receiver calculates the CRC from the data stream and matches it against the CRC

provided by the sender. If the two match, the data has not changed accidentally. This technique is commonly used in network protocols, such as Ethernet.

Parity bits and CRCs protect against accidental modification of data, but do not protect against an attacker. If Alice sends a message to Bob, he can use these techniques as protection against a noisy channel, but a knowledgeable attacker could replace or modify the message without detection.

2.2.2 *Digitized Signatures*

In the paper world, the traditional mechanism for non-repudiation is the handwritten signature. This signature indicates that the signer has written, approved, or acknowledged the contents of the paper document. A digitized signature is sometimes used as a substitute for written signatures when applications are computerized.

A digitized signature is created by scanning in a handwritten signature. When someone wishes to sign an electronic document, they simply insert the image of their signature where appropriate. When the receiver views an electronic document or message, they immediately recognize the meaning of the digitized signature.

Digitized signatures are one of the easiest mechanisms to use. If Bob knows Alice's signature, he will recognize it right away. However, they are also one of the easiest to subvert. Charlie can easily cut Alice's digitized signature from one document and insert it into another. Digitized signatures should not be relied upon for any security services. Digitized signatures are generally used in conjunction with a stronger mechanism to add usability.

2.2.3 *PINs and Passwords*

The traditional method for authenticating users has been to provide them with a personal identification number or secret password, which they must use when requesting access to a particular system. Password systems can be effective if managed properly, but they seldom are. Authentication that relies solely on passwords has often failed to provide adequate protection for computer systems for a number of reasons. If users are allowed to make up their own passwords, they tend to choose ones that are easy to remember and therefore easy to guess. If passwords are generated from a random combination of characters, users often write them down because they are difficult to remember. Where password-only authentication is not adequate for an application, it is often used in combination with other security mechanisms.

PINs and passwords do not provide non-repudiation, confidentiality, or integrity. If Alice wishes to authenticate to Bob using a password, Bob must also know it. Since both Alice and Bob know the password, it is difficult to prove which of them performed a particular operation.

2.2.4 *Biometrics*

Biometric authentication relies on a unique physical characteristic to verify the identity of system users. Common biometric identifiers include fingerprints, written signatures, voice patterns, typing patterns, retinal scans, and hand geometry. The unique pattern that identifies a user is formed during an enrollment process, producing a template for that user.

When a user wishes to authenticate to the system, a physical measurement is made to obtain a current biometric pattern for the user. This pattern can then be compared against the enrollment template in order to verify the user's identity. Biometric authentication devices tend to cost more than password or token-based systems, because the hardware required to capture and analyze biometric patterns is more complicated. However, biometrics provide a very high

level of security because the authentication is directly related to a unique physical characteristic of the user which is more difficult to counterfeit. Recent technological advances have also helped to reduce the cost of biometric authentication systems.

2.2.5 Summary - Non-Cryptographic Security Mechanisms

Non-cryptographic mechanisms may be used to authenticate the identity of a user or verify the integrity of data that has been transmitted over a communications line. None of these mechanisms provide confidentiality or non-repudiation. In general, cryptographic security mechanisms are required to achieve confidentiality or non-repudiation.

Mechanism	Data integrity	Confidentiality	Identification and authentication	Non-repudiation
Parity bits and CRCs	Yes	No	No	No
Digitized signatures	No	No	No	No
PINs and passwords	No	No	Yes	No
Biometrics	No	No	Yes	No

2.3 CRYPTOGRAPHIC SECURITY MECHANISMS

Cryptography is a branch of applied mathematics concerned with transformations of data for security. In cryptography, a sender transforms unprotected information (plaintext) into coded text (ciphertext). A receiver uses cryptography to either (a) transform the ciphertext back into plaintext, (b) verify the sender's identity, (c) verify the data's integrity, or some combination.

In many cases, the sender and receiver will use *keys* as an additional input to the cryptographic algorithm. With some algorithms, it is critical that the keys remain a secret. If Charlie is able to obtain secret keys, he can pretend to be Alice or Bob, or read their private messages. One of the principal problems associated with cryptography is getting secret keys to authorized users without disclosing them to an attacker. This is known as secret key distribution.

This document will examine three commonly used classes of cryptographic mechanisms: symmetric algorithms, secure hash algorithms, and asymmetric algorithms. For each class, we will discuss which of the four security services can be supported. In addition, we will discuss whether the algorithm can be used for secret key distribution.

2.3.1 Symmetric Key

Symmetric key cryptography is a class of algorithms where Alice and Bob share a secret key. These algorithms are primarily used to achieve confidentiality, but may also be used for authentication, integrity and limited non-repudiation.

Symmetric algorithms are ideally suited for confidentiality. Modern symmetric algorithms, such as AES, are very fast and very strong. To use a symmetric algorithm for confidentiality, Alice

transforms a plaintext message to ciphertext using a symmetric algorithm and a key. Alice transmits the ciphertext to Bob. Bob uses the same key to transform the ciphertext back into the plaintext.

Symmetric algorithms can also be used to authenticate the integrity and origin of data. Alice uses her key to generate ciphertext for the entire plaintext, as above. She sends the plaintext and a portion of the ciphertext to Bob. This portion of the ciphertext is known as a message authentication code, or MAC. Bob uses his copy of the key to generate the ciphertext, selects the same portion of the ciphertext and compares it to the MAC he received. If they match, Bob knows that Alice sent him the message. This does not provide non-repudiation, though. Alice can deny sending the message, since Bob could have generated it himself.

Alice and Bob need to share a symmetric key before Alice encrypts or generates a MAC for a message. Establishing that shared key is called **key management**, and it is a difficult problem. Key management can be performed with symmetric key cryptography, but it is a classic "chicken vs. egg" problem. To use symmetric cryptography, Alice and Bob need to share a secret. Once Alice and Bob share a symmetric encryption key, the algorithm can be used to establish additional shared secrets.

In general, that first shared key must be established through "out-of-band" mechanisms. This is acceptable if Alice communicates only with Bob. If she communicates with a larger community, the burden of establishing each relationship becomes a serious impediment to obtaining security services.

However, this problem can become manageable through the introduction of a trusted third party (TTP). If Alice and the party she wishes to communicate with trust the same TTP, they can get a new key for this purpose from the TTP. Each party must establish a secret out of band with the TTP as a starting point. However, Alice will not need to repeat this process for each new party with which she communicates.

2.3.2 Secure Hash

The secure hash function takes a stream of data and reduces it to a fixed size through a one-way mathematical function. The result is called a message digest and can be thought of as a fingerprint of the data. The message digest can be reproduced by any party with the same stream of data, but it is virtually impossible to create a different stream of data that produces the same message digest.

A message digest can be used to provide integrity. If Alice sends a message and its digest to Bob, he can recompute the message digest to protect against accidental changes in the data. However, this does not protect Bob from an attacker. Charlie can intercept Alice's message and replace it with a new message and the digest of the new message.

A secure hash can be used to create a hash-based message authentication code, or HMAC, if Alice and Bob share a secret key. If Alice sends a message and its HMAC to Bob, he can recompute the HMAC to protect against changes in the data from any source. Charlie can intercept Alice's message and replace it with a new message, but he cannot compute an acceptable HMAC without knowing the secret key. If Bob trusts Alice, he may accept an HMAC as authenticating Alice's identity. However, the services of confidentiality and non-repudiation are not provided. The current Federal standard for a secure hash algorithm is SHA-1, which is specified in FIPS 180-1 [NIST 95]. An Internet Engineering Task Force document, RFC 2104 [IETF 99], describes an open specification for HMAC use on the internet. The RFC 2104 HMAC can be used in combination with any iterated cryptographic hash, such as MD5 and SHA-1. It also provides for use of a secret key to calculate and verify the message authentication values.

2.3.3 *Asymmetric (public key) Cryptography*

Asymmetric key cryptography, also known as public key cryptography, uses a class of algorithms in which Alice has a private key, and Bob (and others) have her public key. The public and private keys are generated at the same time, and data encrypted with one key can be decrypted with the other key. That is, a party can encrypt a message using Alice's public key, then only Alice, the owner of the matching private key, can decrypt the message. Asymmetric algorithms are poorly suited for encrypting large messages because they are relatively slow. Instead, these algorithms are used to achieve authentication, integrity and non-repudiation, and support confidentiality through key management. Asymmetric algorithms are used to perform three operations explained below: digital signatures, key transport, and key agreement.

Digital Signatures. Alice can generate a digital signature for a message using a message digest and her private key. To authenticate Alice as the sender, Bob generates the message digest as well and uses Alice's public key to validate the signature. If a different private key was used to generate the signature, the validation will fail.

In contrast to handwritten signatures, a digital signature also verifies the integrity of the data. If the data has been changed since the signature was applied, a different digest would be produced. This would result in a different signature. Therefore, if the data does not have integrity, the validation will fail.

In some circumstances, the digital signature can be used to establish non-repudiation. If Bob can demonstrate that only Alice holds the private key, Alice cannot deny generating the signature. In general, Bob will need to rely on a third party to attest that Alice had the private key.

Digital signatures are also used for authentication to systems or applications. A system can authenticate Alice's identity through a challenge-response protocol. The system generates a random challenge and Alice signs it. If the signature is verified with Alice's public key, it must have been signed by Alice. This type of authentication is useful for remote access to information on a server, protecting network management from masqueraders, or for gaining physical access to a restricted area.

Key Transport. Some asymmetric algorithms (e.g., RSA [RSA 78]) can be used to encrypt and decrypt data. In practice these algorithms are never used to encrypt large amounts of data, because they are much slower than symmetric key algorithms. However, these algorithms are perfectly suited to encrypting small amounts of data – such as a symmetric key. This operation is called key transport or key exchange, and is used in many protocols. The following example might describe an electronic mail message from Alice to Bob:

- Alice generates an AES [NIST 01b] key, and encrypts the message. She encrypts the AES key using Bob's public key, and sends both the encrypted key and encrypted message to Bob.
- Bob uses his private key to recover Alice's AES key; he then uses the AES key to obtain the plaintext message.

In this case, Alice uses asymmetric cryptography to achieve confidentiality for key distribution. This procedure does not provide any additional security services; since Alice used Bob's public key, anyone could have generated the message.

Key Agreement. Other asymmetric algorithms (e.g., Diffie-Hellman [DH 76]) may be used for key agreement. Assume Bob and Alice each generated a pair of Diffie-Hellman keys. Alice has her private key and Bob's public key. Bob has his private key and Alice's public key. Through a mathematical algorithm, Alice and Bob both generate the same secret value. Charlie may have both public keys, but he cannot calculate the secret value. Alice and Bob can use the secret value that they independently calculated as the AES key and protect their messages.

There are forms of key agreement that provide implicit authentication as well. If Bob can retrieve the plaintext, he knows it was encrypted by Alice. She is the only one that could have generated the same secret value.

2.3.4 Summary – Cryptographic Mechanisms

Cryptographic mechanisms need to be used in concert to provide a complete suite of security services. Each class of algorithms has strengths and weaknesses.

Symmetric cryptographic algorithms, such as AES, are needed to achieve confidentiality. These algorithms can provide some degree of integrity and authentication as well, but they are poorly suited to achieve non-repudiation. The Achilles heel for symmetric algorithms, however, is key distribution.

The secure hash algorithm and the HMAC provide the basis for data integrity in electronic communications. They do not provide confidentiality, and are a weak tool for authentication or non-repudiation. The secure hash and HMAC cannot be used for key distribution, either.

Symmetric cryptographic algorithms are highly effective for integrity, authentication, and key distribution. Digital signature algorithms, such as RSA or DSA, leverage secure hash algorithms for efficiency. When leveraging a trusted third party, digital signatures can be used to provide non-repudiation. Key transport algorithms (e.g., RSA) and key agreement algorithms (e.g., Diffie-Hellman) can be used to efficiently and securely distribute symmetric keys. Once again, leveraging a trusted third party to establish the identity of the private key holder simplifies the problem.

Many applications will use these three classes of cryptographic mechanisms in concert to achieve the complete suite of security services.

Mechanism		Data integrity	Confidentiality	Identification and authentication	Non-repudiation	Key Distribution
Symmetric key cryptography	Encryption	No	Yes	No	No	No
	Message authentication codes	Yes	No	Yes	No	No
	Key transport	No	No	No	No	Yes-requires out-of-band initialization step or a TTP
Secure Hash Functions	Message digest	Yes	No	No	No	No
	HMAC	Yes	No	Yes	No	No
Asymmetric cryptography	Digital signatures	Yes	No	Yes	Yes (with a TTP)	No
	Key transport	No	No	No	No	Yes
	Key Agreement	No	No	Yes	No	Yes

2.4 Security Infrastructures

To achieve the broad range of security services, Alice and Bob will need to use several classes of cryptographic security mechanisms in concert. In particular, to achieve confidentiality they will need to distribute symmetric encryption keys. Distributing symmetric keys can be performed three ways: (1) directly between the parties using symmetric encryption; (2) using symmetric encryption and a trusted third party (TTP); or (3) using public key based key management with a TTP.

The first mechanism is sufficient for small closed communities. If Alice communicates with just three or four people, she can perform an out-of-band initialization with each party. As communities grow, this solution fails to scale, though. What if Alice communicates with dozens of people? Now she needs a TTP to eliminate the out-of-band initialization step. The second mechanism is clearly more scalable, but it provides only limited support for authentication and does not support non-repudiation.

The third mechanism is also scalable, and it also provides a comprehensive solution. If a TTP binds the public key to a user or system – that is, attests to the identity of the party holding the corresponding private key - the complete range of security services may be obtained. The user may obtain integrity, authentication, and non-repudiation through digital signatures. Symmetric

keys can be distributed using either key transport or key agreement. Those symmetric keys can be used to achieve confidentiality.

Of course, a single TTP will only scale so far. To achieve security services across organizational boundaries, many inter-linked TTPs will be required. This set of interlinked TTPs forms a security infrastructure that users can rely upon to obtain security services. When this security infrastructure is designed to distribute public keys, it is known as a public key infrastructure (PKI).

3 PUBLIC KEY INFRASTRUCTURES

A public key infrastructure (PKI) binds public keys to entities, enables other entities to verify public key bindings, and provides the services needed for ongoing management of keys in a distributed system.

The overall goals of modern security architectures are to protect and distribute information that is needed in a widely distributed environment, where the users, resources and stake-holders may all be in different places at different times. The emerging approach to address these security needs makes use of the scalable and distributed characteristics of public key infrastructure ("PKI"). PKI allows you to conduct business electronically with the confidence that:

- The person or process identified as sending the transaction is actually the originator.
- The person or process receiving the transaction is the intended recipient.
- Data integrity has not been compromised.

In conventional business transactions, customers and merchants rely on credit cards (e.g., VISA or MasterCard) to complete the financial aspects of transactions. The merchant may authenticate the customer through signature comparison or by checking identification, such as a driver's license. The merchant relies on the information on the credit card and status information obtained from the credit card issuer to ensure that payment will be received. Similarly, the customer performs the transaction knowing they can reject the bill if the merchant fails to provide the goods or services. The credit card issuer is the trusted third party in this type of transaction.

The same model is often applied in electronic commerce, even though the customer and issuer may never meet. The merchant cannot check the signature or request identification information. At best, the merchant can verify the customer's address against the credit card issuer's database. Again, the customer knows that they can reject the bill if the merchant fails to provide the goods or services. The credit card issuer is the trusted third party that makes consumer-to-business e-commerce possible.

With electronic commerce, customer and merchant may be separated by hundreds of miles. Other forms of authentication are needed, and the customer's credit card and financial information must be protected for transmission over the internet. Customers who do business with a merchant over the internet must use encryption methods that enable them to protect the information they transmit to the merchant, and the merchant must protect the information it transmits back to customers. Both customer and merchant must be able to obtain encryption keys and ensure that the other party is legitimate. The PKI provides the mechanisms to accomplish these tasks.

Two parties who wish to transact business securely may be separated geographically, and may not have ever met. To use public key cryptography to achieve their security services, they must be able to obtain each other's public keys and authenticate the other party's identity. This may be performed out-of-band if only two parties need to conduct business. If they will conduct business with a variety of parties, or cannot use out-of-band means, they must rely on a trusted third party to distribute the public keys and authenticate the identity of the party associated with the corresponding key pair.

Public key infrastructure is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on networks. PKI integrates digital certificates, public key cryptography, and certification authorities into a complete enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers;

end-user enrollment software; integration with certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

The term public key infrastructure is derived from public key cryptography, the technology on which PKI is based. Public key cryptography is the technology behind modern digital signature techniques. It has unique features that make it invaluable as a basis for security functions in distributed systems. This section provides additional background on the underlying mechanisms of a public key system.

3.1 PKI COMPONENTS

Functional elements of a public key infrastructure include certification authorities, registration authorities, repositories, and archives. The users of the PKI come in two flavors: certificate holders and relying parties. An attribute authority is an optional component.

A **certification authority (CA)** is similar to a notary. The CA confirms the identities of parties sending and receiving electronic payments or other communications. Authentication is a necessary element of many formal communications between parties, including payment transactions. In most check-cashing transactions, a driver's license with a picture is sufficient authentication. A personal identification number (PIN) provides electronic authentication for transactions at a bank automated teller machine (ATM).

A **registration authority (RA)** is an entity that is trusted by the CA to register or vouch for the identity of users to a CA.

A **repository** is a database of active digital certificates for a CA system. The main business of the repository is to provide data that allows users to confirm the status of digital certificates for individuals and businesses that receive digitally signed messages. These message recipients are called relying parties. CAs post certificates and CRLs to repositories.

An **archive** is a database of information to be used in settling future disputes. The business of the archive is to store and protect sufficient information to determine if a digital signature on an "old" document should be trusted.

The CA issues a **public key certificate** for each identity, confirming that the identity has the appropriate credentials. A digital certificate typically includes the public key, information about the identity of the party holding the corresponding private key, the operational period for the certificate, and the CA's own digital signature. In addition, the certificate may contain other information about the signing party or information about the recommended uses for the public key. A subscriber is an individual or business entity that has contracted with a CA to receive a digital certificate verifying an identity for digitally signing electronic messages.

CAs must also issue and process **certificate revocation lists (CRLs),** which are lists of certificates that have been revoked. The list is usually signed by the same entity that issued the certificates. Certificates may be revoked, for example, if the owner's private key has been lost; the owner leaves the company or agency; or the owner's name changes. CRLs also document the historical revocation status of certificates. That is, a dated signature may be presumed to be valid if the signature date was within the validity period of the certificate, and the current CRL of the issuing CA at that date did not show the certificate to be revoked.

PKI users are organizations or individuals that use the PKI, but do not issue certificates. They rely on the other components of the PKI to obtain certificates, and to verify the certificates of other entities that they do business with. End entities include the *relying party*, who relies on the certificate to know, with certainty, the public key of another entity; and the *certificate holder*, that is issued a certificate and can sign digital documents. Note that an individual or organization may be both a relying party and a certificate holder for various applications.

3.1.1 Certification Authorities

The certification authority, or CA, is the basic building block of the PKI. The CA is a collection of computer hardware, software, and the people who operate it. The CA is known by two attributes: its name and its public key. The CA performs four basic PKI functions: issues certificates (i.e., creates and signs them); maintains certificate status information and issues CRLs; publishes its current (e.g., unexpired) certificates and CRLs, so users can obtain the information they need to implement security services; and maintains archives of status information about the expired certificates that it issued. These requirements may be difficult to satisfy simultaneously. To fulfill these requirements, the CA may delegate certain functions to the other components of the infrastructure.

A CA may issue certificates to users, to other CAs, or both. When a CA issues a certificate, it is asserting that the subject (the entity named in the certificate) has the private key that corresponds to the public key contained in the certificate. If the CA includes additional information in the certificate, the CA is asserting that information corresponds to the subject as well. This additional information might be contact information (e.g., an electronic mail address), or policy information (e.g., the types of applications that can be performed with this public key.) When the subject of the certificate is another CA, the issuer is asserting that the certificates issued by the other CA are trustworthy.

The CA inserts its name in every certificate (and CRL) it generates, and signs them with its private key. Once users establish that they trust a CA (directly, or through a certification path) they can trust certificates issued by that CA. Users can easily identify certificates issued by that CA by comparing its name. To ensure the certificate is genuine, they verify the signature using the CA's public key. As a result, it is important that the CA provide adequate protection for its own private key. Federal government CAs should always use cryptographic modules that have been validated against FIPS 140.

As CA operation is central to the security services provided by a PKI, this topic is explored in additional detail in Section 5, CA System Operation.

3.1.2 Registration Authorities

An RA is designed to verify certificate contents for the CA. Certificate contents may reflect information presented by the entity requesting the certificate, such as a drivers license or recent pay stub. They may also reflect information provided by a third party. For example, the credit limit assigned to a credit card reflects information obtained from credit bureaus. A certificate may reflect data from the company's Human Resources department, or a letter from a designated company official. For example, Bob's certificate could indicate that he has signature authority for small contracts. The RA aggregates these inputs and provides this information to the CA.

Like the CA, the RA is a collection of computer hardware, software, and the person or people who operate it. Unlike a CA, an RA will often be operated by a single person. Each CA will maintain a list of accredited RAs; that is a list of RAs determined to be trustworthy. An RA is known to the CA by a name and a public key. By verifying the RA's signature on a message, the CA can be sure an accredited RA provided the information, and it can be trusted. As a result, it is important that the RA provide adequate protection for its own private key. Federal government RAs should always use cryptographic modules that have been validated against FIPS 140.

3.1.3 PKI Repositories

PKI applications are heavily dependent on an underlying directory service for the distribution of certificates and certificate status information. The directory provides a means of storing and distributing certificates, and managing updates to certificates. Directory servers are typically implementations of the X.500 standard or subset of this standard.

X.500 consists of a series of recommendations and the specification itself references several ISO standards. It was designed for directory services that could work across system, corporate, and international boundaries. A suite of protocols is specified for operations such as chaining, shadowing, and referral for server-to-server communication, and the Directory Access Protocol (DAP) for client to server communication. The Lightweight Directory Access Protocol (LDAP) was later developed as an alternative to DAP. Most directory servers and clients support LDAP, though not all support DAP.

To be useful for the PKI applications, directory servers need to be interoperable; without such interoperability, a relying party will not be able to retrieve the needed certificates and CRLs from remote sites for signature verifications. To promote interoperablility among Federal agency directories and thus PKI deployments, the Federal PKI Technical Working Group is developing a Federal PKI Directory Profile [Chang] to assist agencies interested in participating in the FBCA demonstration effort. It is recommended that agencies refer to this document for the minimum interoperability requirements before standing up their agency directories.

3.1.4 Archives

An archive accepts the responsibility for long term storage of archival information on behalf of the CA. An archive asserts that the information was good at the time it was received, and has not been modified while in the archive. The information provided by the CA to the archive must be sufficient to determine if a certificate was actually issued by the CA as specified in the certificate, and valid at that time. The archive protects that information through technical mechanisms and appropriate procedures while in its care. If a dispute arises at a later date, the information can be used to verify that the private key associated with the certificate was used to sign a document. This permits the verification of signatures on old documents (such as wills) at a later date.

3.1.5 PKI users

PKI Users are organizations or individuals that use the PKI, but do not issue certificates. They rely on the other components of the PKI to obtain certificates, and to verify the certificates of other entities that they do business with. End entities include the relying party, who relies on the certificate to know, with certainty, the public key of another entity; and the certificate holder, that is issued a certificate and can sign digital documents. Note that an individual or organization may be both a relying party and a certificate holder for various applications.

3.2 PKI Architectures

Certificate holders will obtain their certificates from different CAs, depending upon the organization or community in which they are a member. A PKI is typically composed of many CAs linked by trust paths. A trust path links a relying party with one or more trusted third parties, such that the relying party can have confidence in the validity of the certificate in use. Recipients of a signed message who have no relationship with the CA that issued the certificate for the

sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate.

The initial challenge is deploying a PKI that can be used throughout an enterprise (e.g., a company or government agency). There are two traditional PKI architectures to support this goal, **hierarchical** and **mesh** enterprise architectures. More recently, enterprises are seeking to link their own PKIs to those of their business partners. A third approach, **bridge CA** architecture, has been developed to address this problem. These three architectures are described below.

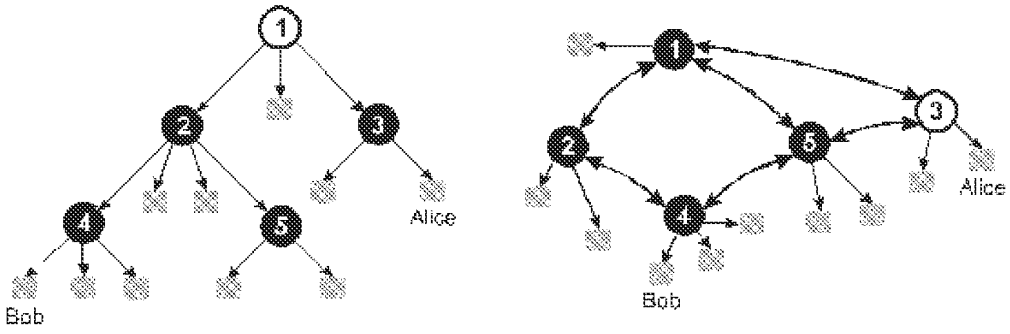
3.2.1 Enterprise PKI Architectures

CAs may be linked in a number of ways. Most enterprises that deploy a PKI will choose either a "mesh" or a "hierarchical" architecture:

- *Hierarchical:* Authorities are arranged hierarchically under a "root" CA that issues certificates to subordinate CAs. These CAs may issue certificates to CAs below them in the hierarchy, or to users. In a hierarchical PKI, every relying party knows the public key of the root CA. Any certificate may be verified by verifying the certification path of certificates from the root CA. Alice verifies Bob's certificate, issued by CA 4, then CA 4's certificate, issued by CA 2, and then CA 2's certificate issued by CA 1, the root, whose public key she knows.

- *Mesh*: Independent CA's cross certify each other (that is issue certificates to each other), resulting in a general mesh of trust relationships between peer CAs. Figure 1 (b) illustrates a mesh of authorities. A relying party knows the public key of a CA "near" himself, generally the one that issued his certificate. The relying party verifies certificate by verifying a certification path of certificates that leads from that trusted CA. CAs cross certify with each other, that is they issue certificates to each other, and combine the two in a **crossCertificatePair**. So, for example, Alice knows the public key of CA 3, while Bob knows the public key of CA 4. There are several certification paths that lead from Bob to Alice. The shortest requires Alice to verify Bob's certificate, issued by CA 4, then CA 4's certificate issued by CA 5 and finally CA 5's certificate, issued by CA 3. CA 3 is Alice's CA and she trusts CA 3 and knows its public key.

Figure 1 illustrates these two basic PKI architectures.



a. hierarchical infrastructure b. mesh infrastructure

Figure 1. Traditional PKI Architectures

3.2.2 *Bridge PKI Architecture*

The Bridge CA architecture was designed to connect enterprise PKIs regardless of the architecture. This is accomplished by introducing a new CA, called a Bridge CA, whose sole purpose is to establish relationships with enterprise PKIs.

Unlike a mesh CA, the Bridge CA does not issue certificates directly to users. Unlike a root CA in a hierarchy, the Bridge CA is not intended for use as a trust point. All PKI users consider the Bridge CA an intermediary. The Bridge CA establishes peer-to-peer relationships with different enterprise PKIs. These relationships can be combined to form a bridge of trust connecting the users from the different PKIs.

If the trust domain is implemented as a hierarchical PKI, the Bridge CA will establish a relationship with the root CA. If the domain is implemented as a mesh PKI, the bridge will establish a relationship with only one of its CAs. In either case, the CA that enters into a trust relationship with the Bridge is termed a principal CA.

In Figure 2, the Bridge CA has established relationships with three enterprise PKIs. The first is Bob's and Alice's CA, the second is Carol's hierarchical PKI, and the third is Doug's mesh PKI. None of the users trusts the Bridge CA directly. Alice and Bob trust the CA that issued their certificates; they trust the Bridge CA because the Fox CA issued a certificate to it. Carol's trust point is the root CA of her hierarchy; she trusts the Bridge CA because the root CA issued a certificate to it. Doug trusts the CA in the mesh that issued his certificate; he trusts the Bridge CA because there is a valid certification path from the CA that issued him a certificate to the Bridge CA. Alice (or Bob) can use the bridge of trust that exists through the Bridge CA to establish relationships with Carol and Doug.

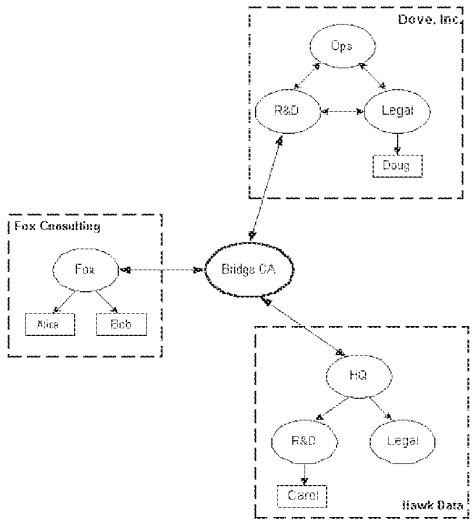


Figure 2. Bridge CA and Enterprise PKIs

3.2.3 *Physical Architecture*

There are numerous ways in which a PKI can be designed physically. It is highly recommended that the major PKI components be implemented on separate systems, that is, the CA on one system, the RA on a different system, and directory servers on other systems. Because the systems contain sensitive data, they should be located behind an organization's Internet firewall.

The CA system is especially important because a compromise to that system could potentially disrupt the entire operations of the PKI and necessitate starting over with new certificates. Consequently, placing the CA system behind an additional organizational firewall is recommended so that it is protected both from the Internet and from systems in the organization itself. Of course, the organizational firewall would permit communications between the CA and the RA as well as other appropriate systems.

If distinct organizations wish to access certificates from each other, their directories will need to be made available to each other and possibly to other organizations on the Internet. However, some organizations will use the directory server for much more than simply a repository for certificates. The directory server may contain other data considered sensitive to the organization and thus the directory may be too sensitive to be made publicly available. A typical solution would be to create a directory that contains only the public keys or certificates, and to locate this directory at the border of the organization - this directory is referred to as a **border directory**. A likely location for the directory would be outside the organization's firewall or perhaps on a protected DMZ segment of its network so that it is still available to the public but better protected from attack. Figure 3 illustrates a typical arrangement of PKI-related systems.

The main directory server located within the organization's protected network would periodically refresh the border directory with new certificates or updates to the existing certificates. Users within the organization would use the main directory server, whereas other systems and organizations would access only the border directory. When a user in organization A wishes to send encrypted e-mail to a user in organization B, user A would then retrieve user B's certificate from organization B's border directory, and then use the public key in that certificate to encrypt the e-mail.

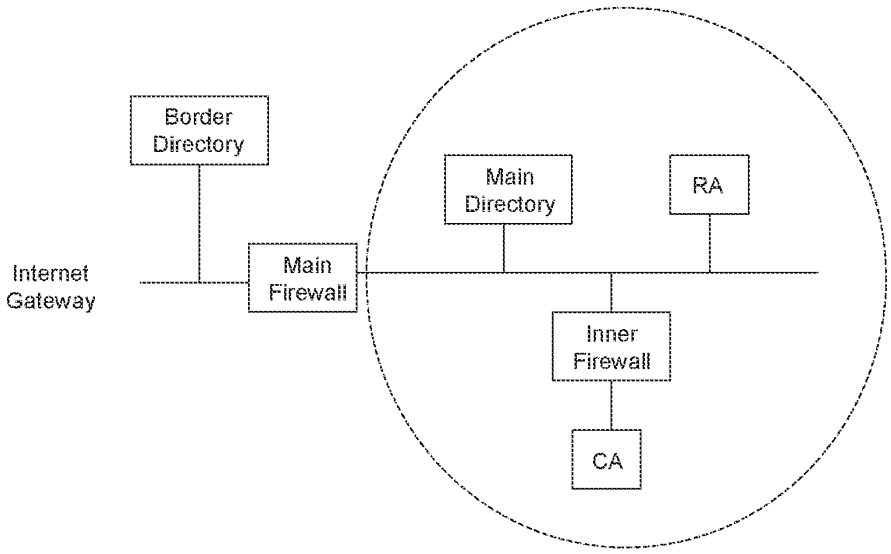


Figure 3. PKI Physical Topology

3.3 PKI Data Structures

Two basic data structures are used in PKIs. These are the **public key certificate** and the **certificate revocation lists**. A third data structure, the **attribute certificate**, may be used as an addendum

3.3.1 X.509 Public Key Certificates

The X.509 public key certificate format [IETF 01] has evolved into a flexible and powerful mechanism. It may be used to convey a wide variety of information. Much of that information is optional, and the contents of mandatory fields may vary as well. It is important for PKI implementers to understand the choices they face, and their consequences. Unwise choices may hinder interoperability or prevent support for critical applications.

The X.509 public key certificate is protected by a digital signature of the issuer. Certificate users know the contents have not been tampered with since the signature was generated if the signature can be verified. Certificates contain a set of common fields, and may also include an optional set of extensions.

There are ten common fields: six mandatory and four optional. The mandatory fields are: the serial number, the certificate signature algorithm identifier, the certificate issuer name, the certificate validity period, the public key, and the subject name. The subject is the party that controls the corresponding private key. There are four optional fields: the version number, two unique identifiers, and the extensions. These optional fields appear only in version 2 and 3 certificates.

Version. The version field describes the syntax of the certificate. When the version field is omitted, the certificate is encoded in the original, version 1, syntax. Version 1 certificates do not include the unique identifiers or extensions. When the certificate includes unique identifiers but not extensions, the version field indicates version 2. When the certificate includes extensions, as almost all modern certificates do, the version field indicates version 3.

Serial number. The serial number is an integer assigned by the certificate issuer to each certificate. The serial number must be unique for each certificate generated by a particular issuer. The combination of the issuer name and serial number uniquely identifies any certificate.

Signature. The signature field indicates which digital signature algorithm (e.g., DSA with SHA-1 or RSA with MD5) was used to protect the certificate.

Issuer. The issuer field contains the X.500 distinguished name of the TTP that generated the certificate.

Validity. The validity field indicates the dates on which the certificate becomes valid and the date on which the certificate expires.

Subject. The subject field contains the distinguished name of the holder of the private key corresponding to the public key in this certificate. The subject may be a CA, a RA, or an end entity. End entities can be human users, hardware devices, or anything else that might make use of the private key.

Subject public key information. The subject public key information field contains the subject's public key, optional parameters, and algorithm identifier. The public key in this field, along with the optional algorithm parameters, is used to verify digital signatures or perform key management. If the certificate subject is a CA, then the public key is used to verify the digital signature on a certificate.

Issuer unique ID and **subject unique ID**. These fields contain identifiers, and only appear in version 2 or version 3 certificates. The subject and issuer unique identifiers are intended to handle the reuse of subject names or issuer names over time. However, this mechanism has proven to be an unsatisfactory solution. The Internet Certificate and CRL profile does not [HOUS99] recommend inclusion of these fields.

Extensions. This optional field only appears in version 3 certificates. If present, this field contains one or more certificate extensions. Each extension includes an extension identifier, a criticality flag, and an extension value. Common certificate extensions have been defined by ISO and ANSI to answer questions that are not satisfied by the common fields.

Subject type. This field indicates whether a subject is a CA or an end entity.

Names and identity information. This field aids in resolving questions about a user's identity, e.g., are "alice@gsa.gov" and "c=US; o=U.S. Government; ou=GSA; cn=Alice Adams" the same person?

Key attributes. This field specifies relevant attributes of public keys, e.g., whether it can be used for key transport, or be used to verify a digital signature.

Policy information. This field helps users determine if another user's certificate can be trusted, whether it is appropriate for large transactions, and other conditions that vary with organizational policies.

Certificate extensions allow the CA to include information not supported by the basic certificate content. Any organization may define a private extension to meet its particular business requirements. However, most requirements can be satisfied using standard extensions. Standard extensions are widely supported by commercial products. Standard extensions offer improved interoperability, and they are more cost effective than private extensions.

Extensions have three components: **extension identifier**, a **criticality flag**, and **extension value**. The extension identifier indicates the format and semantics of the extension value. The criticality flag indicates the importance of the extension. When the criticality flag is set, the information is essential to certificate use. Therefore, if an unrecognized critical extension is encountered, the certificate must not be used. Alternatively, an unrecognized non-critical extension may be ignored.

The subject of a certificate could be an end user or another CA. The basic certificate fields do not differentiate between these types of users. The **basic constraints** extension appears in CA certificates, indicating this certificate may be used to build certification paths.

The **key usage** extension indicates the types of security services that this public key can be used to implement. These may be generic services (e.g., non-repudiation or data encryption) or PKI specific services (e.g., verifying signatures on certificates or CRLs).

The subject field contains a directory name, but that may not be the type of name that is used by a particular application. The **subject alternative name** extension is used to provide other name forms for the owner of the private key, such as DNS names or email addresses. For example, the email address alice@gsa.gov.gov could appear in this field.

CAs may have multiple key pairs. The **authority key identifier** extension helps users select the right public key to verify the signature on this certificate.

Users may also have multiple key pairs, or multiple certificates for the same key. The **subject key identifier** extension is used to identify the appropriate public key.

Organizations may support a broad range of applications using PKI. Some certificates may be more trustworthy than others, based on the procedures used to issue them or the type of user cryptographic module. The **certificate policies** extension contains a globally unique identifier that specifies the certificate policy that applies to this certificate.

Different organizations (e.g., different companies or government agencies) will use different certificate policies. Users will not recognize policies from other organizations. The **policy mappings** extension converts policy information from other organizations into locally useful policies. This extension appears only in CA certificates.

The CRL **distribution points** extension contains a pointer to the X.509 CRL where status information for this certificate may be found. (X.509 CRLs are described in the following section.)

When a CA issues a certificate to another CA, it is asserting that the other CA's certificates are trustworthy. Sometimes, the issuer would like to assert that a subset of the certificates should be trusted. There are three basic ways to specify that a subset of certificates should be trusted:

The **basic constraints** extension (described above) has a second role, indicating whether this CA is trusted to issue CA certificates, or just user certificates.

The **name constraints** extension can be used to describe a subset of certificates based on the names in either the subject or subject alternative name fields. This extension can be used to define the set of acceptable names, or the set of unacceptable names. That is, the CA could assert "names in the NIST directory space are acceptable" or "names in the NIST directory space are *not* acceptable."

The **policy constraints** extension can be used to describe a subset of certificates based on the contents of the policy extension. If policy constraints are implemented, users will reject certificates without a policy extension, or where the specified policies are unrecognized.

3.3.2 Certificate Revocation Lists (CRLs)

Certificates contain an expiration date. Unfortunately, the data in a certificate may become unreliable before the expiration date arrives. Certificate issuers need a mechanism to provide a status update for the certificates they have issued. One mechanism is the X.509 certification revocation list (CRL).

CRLs are the PKI analog of the credit card hot list that store clerks review before accepting large credit card transactions. The CRL is protected by a digital signature of the CRL issuer. If the signature can be verified, CRL users know the contents have not been tampered with since the signature was generated. CRLs contain a set of common fields, and may also include an optional set of extensions.

The CRL contains the following fields:

Version. The optional version field describes the syntax of the CRL. (In general, the version will be two.)

Signature. The signature field contains the algorithm identifier for the digital signature algorithm used by the CRL issuer to sign the CRL.

Issuer. The issuer field contains the X.500 distinguished name of the CRL issuer.

This update. The this-update field indicates the issue date of this CRL.

Next update. The next-update field indicates the date by which the next CRL will be issued.

Revoked certificates. The revoked certificates structure lists the revoked certificates. The entry for each revoked certificate contains the certificate serial number, time of revocation, and optional CRL entry extensions.

The CRL entry extensions field is used to provide additional information about this particular revoked certificate. This field may only appear if the version is v2.

CRL Extensions. The CRL extensions field is used to provide additional information about the whole CRL. Again, this field may only appear if the version is v2.

ITU-T and ANSI X9 have defined several CRL extensions for X.509 v2 CRLs. They are specified in [X509 97] and [X955]. Each extension in a CRL may be designated as critical or non-critical. A CRL validation fails if an unrecognized critical extension is encountered. However, unrecognized non-critical extensions may be ignored. The X.509 v2 CRL format allows communities to define private extensions to carry information unique to those communities. Communities are encouraged to define non-critical private extensions so that their CRLs can be readily validated by all implementations.

The most commonly used CRL extensions include the following:

The **CRL number** extension is essentially a counter. In general, this extension is provided so that users are informed if an emergency CRL was issued.

As noted in the previous section, CAs may have multiple key pairs. When appearing in a CRL, the **authority key identifier** extension helps users select the right public key to verify the signature on this CRL.

The issuer field contains a directory name, but that may not be the type of name that is used by a particular application. The **issuer alternative name** extension is used to provide other name forms for the owner of the private key, such as DNS names or email addresses. For example, the email address CA1@nist.gov could appear in this field.

The **issuing distribution points** extension is used in conjunction with the CRL distribution points extension in certificates. This extension is used to confirm that this particular CRL is the one described by the CRL distribution points extension and contains status information for certificate in question. This extension is required when the CRL does not cover all certificates issued by a CA, since the CRL may be distributed on an insecure network.

The extensions described above apply to the entire CRL. There are also extensions that apply to a particular revoked certificate.

Certificates may be revoked for a number of different reasons. The user's crypto module may have been stolen, for example, or the module may simply have been broken. The **reason code** extension describes why a particular certificate was revoked. The relying party may use this information to decide if a previously generated signature may be accepted.

Sometimes a CA does not wish to issue its own CRLs. It may delegate this task to another CA. The CA that issues a CRL may include the status of certificates issued by a number of different CAs in the same CRL. The **certificate issuer** extension is used to specify which CA issued a particular certificate, or set of certificates, on a CRL.

3.3.3 Attribute Certificates

The public key certificates described in 3.1.1 are focused on the binding between the subject and the public key. The relationship between the subject and public key is expected to be a long-lived relationship. Most end entity certificates include a validity period of a year or two years.

Organizations seek improved access control. Public key certificates can be used to authenticate the identity of a user, and this identity can be used as an input to access control decision functions. However, in many contexts, the identity is not the criterion used for access control decisions. The access control decision may depend upon role, security clearance, group membership, or ability to pay.

Authorization information, such as membership in a group, often has a shorter lifetime than the binding of the identity and the public key. Authorization information could be placed in a public key certificate extension. However, this is not a good strategy for two reasons. First, the certificate is likely to be revoked because the authorization information needs to be updated. Revoking and reissuing the public key certificate with updated authorization information is quite expensive. Second, the CA that issues public key certificates is not likely to be authoritative for the authorization information. This results in additional steps for the CA to contact the authoritative authorization information source.

The X.509 attribute certificate (AC) binds attributes to an AC **holder** [X509 97]. This definition is being profiled for use in Internet applications. Since the AC does not contain a public key, the AC is used in conjunction with a public key certificate. An access control function may make use of the attributes in an AC, but it is not a replacement for authentication. The public key certificate must first be used to perform authentication, then the AC is used to associate attributes with the authenticated identity.

ACs may also be used in the context of a data origin authentication service and a non-repudiation service. In these contexts, the attributes contained in the AC provide additional information about the signing entity. This information can be used to make sure that the entity is authorized to sign the data. This kind of checking depends either on the context in which the data is exchanged or on the data that has been digitally signed.

An X.509 AC resembles the X.509 public key certificate. The AC is an ASN.1 DER encoded object, and is signed by the issuer. An AC contains nine fields: version, holder, issuer, signature algorithm identifier, serial number, validity period, attributes, issuer unique identifier, and extensions. The AC holder is similar to the public key certificate subject, but the holder may be specified with a name, the issuer and serial number of a public key certificate, or the one-way hash of a certificate or public key. The attributes describe the authorization information associated with the AC holder. The extensions describe additional information about the certificate and how it may be used.

3.4 ADDITIONAL PKI SERVICES

In addition to the security services described previously (non-repudiation, identification and authentication, confidentiality and integrity), PKIs can also offer other services. Two important services that may be offered by a PKI are key recovery and authorization. These services are described below.

Key Recovery. If a user's key is lost, agencies and businesses must still be able to recover data that the employee had encrypted, which can only be done by recovering the encryption key. Reasons for key recovery may include an employee forgetting a password to unlock an encrypted file, the death of an employee who has encrypted some information, or someone attempting to hide criminal activity from law enforcement officials. To ensure the ability to recover encrypted data, encryption keys must be backed up and stored securely.

Note, however, that *signing* keys, i.e., keys used for digital signatures, should not be backed up, since doing so prevents the PKI from ensuring non-repudiation. If anyone other than a particular user has a copy of a signing key, then that user can claim that someone else supplied the signature on a contested document. If a user loses a signing key, a new key and associated certificate can be easily generated. The PKI must keep track of the user's possession of a key, but not the key itself.

Privilege/Authorization. Certificates can be used to vouch for a user's identity and also specify privileges the user has been granted. Privileges might include authority to view classified information or permission to modify material on a Web server among other privileges.

3.5 Case Study

A PKI can support a wide variety of internet and e-commerce applications, including secure electronic mail, virtual private networks, secure web access, and custom applications. The following procurement example illustrates how the services listed above are achieved, and the role played by the major PKI components. For the purposes of this example, we will assume RSA for signatures and key transport, SHA-1 for the hash, and AES for encryption.

Alice is a buyer for the Alpha company. She wishes to obtain widgets from the Beta corporation for Alpha's new product line. The Alpha company does not want its competitors to know anything about the new products – not even that widgets are a subcomponent. Alice wishes to negotiate with Bob, the head of sales at Beta, electronically.

Alice generates two public-private key pairs, one for signature the other for encryption. She goes to the Alpha company RA and provides the signature public key and a valid Alpha company photo-id. The RA verifies the buyer's identity based on the photo-id and vouches for the identity of the buyer to Alpha's CA, who then issues the signature certificate to Alice. The Alpha CA posts the new certificate in the Alpha company directory. Alice returns to her desk and uses her signature to authenticate her request for a key exchange certificate. In this request, Alice provides both her public and private encryption keys. The Alpha CA issues a key transport certificate to Alice and escrows her encryption private key. The Alpha CA also periodically posts a CRL.

The Beta corporation also has a CA. Bob has previously generated his key pairs and obtained certificates. The Beta CA has posted the certificates to its directory. Like the Alpha CA, the Beta CA posts CRLs as well.

Alice constructs a message describing the number of widgets she needs and the schedule for delivery. She signs the message using the private key associated with the public key in her signing certificate. She generates an AES key and encrypts the message. Next, Alice obtains Bob's key transport public key from the Beta directory. Alice verifies that this certificate has not been revoked, and encrypts her AES key using Bob's public key. Alice sends Bob the signed and encrypted message along with the encrypted AES key.

Bob uses his key transport private key to decrypt encrypted AES key. He then uses the AES key to decrypt the message. Now he can read the contents, but is unsure if it really originated from Alice or if it has been changed since Alice created it. Bob obtains Alice's signature certificate from the Alpha directory along with the current CRL. After verifying the certificate has

not been revoked, Bob can verify the digital signature on the message. If the signature validates, Bob knows the message came from Alice and has not been modified. He can concentrate on providing an accurate quote to the Alpha company.

Alice and Bob negotiate a deal and the widgets are delivered. The bill arrives, and the Alpha company disputes the cost. This dispute must be settled immediately, or the new product line will be delayed. The CEO needs to see the messages Bob sent to Alice. Unfortunately, Alice is on an adventure vacation and cannot be contacted, so she can not decrypt the messages. The CEO of the Alpha company requests Alice's private encryption key from the escrow server. After determining the request is authentic, the key is returned to the CEO. The CEO uses the key to decrypt the message from the negotiation between Alice and Bob, and the dispute is settled.

We could extend this scenario further to include attribute certificates for authorization. The attribute authority would have issued an attribute certificate to the CEO authorizing him to perform key recovery operations. The escrow server would retrieve and verify the CEO's attribute certificate before approving the escrow request.

4 Issues and Risks in CA System Operation

To issue digital certificates, a CA must verify subscribers' identities; determine the appropriate content of digital certificates; create, distribute, and ensure acceptance of digital certificates; and ensure internal security. Each of these actions introduces some risk to the parties involved. This section discusses some of these risks and tradeoffs that can be made to reduce or spread the risk[1].

CA systems may be characterized as primarily open or closed. A fully closed system has contracts defining the rights and obligations of all participants for authenticating messages or transactions. This type of system offers the CA operators less risk exposure because there is little uncertainty regarding obligations. Conversely, a fully open system would not have formal contracts defining the rights and obligations of relying parties in the system. In such a system, the firms that perform the CA activities could be exposed to an uncertain level of risk for each authenticated message or transaction. It is likely during early stages of development that most CA systems will be neither fully open nor fully closed, with contracts defining the rights and responsibilities of at least some, but not all, of the system participants.

4.1 Verifying Identity

To confirm the identity of a subscriber, the CA either reviews the subscriber's credentials internally or contracts with a registration authority (RA). The decision to outsource and the choice of RA expose the CA to risk. If the CA or RA confirms an identity that is false, or somehow inaccurate, the CA may suffer loss of business or even expose itself to legal actions. Moreover, the CA's outstanding certificates may become suspect if there is a pattern of insufficient due diligence in verifying identities for issuing certificates. The risk exposure from falsely identifying a subscriber may be reduced when a CA issues digital certificates for use within a closed system, because there are contracts in place between some or all of the participants in the system.

4.2 Certificate Content

Certificates' content varies by CA system. Content and a certificate's limitations are a source of strategic risk to the issuing CA. Standard certificates identify the subscriber and the issuing CA. Another important element of a standard certificate is the expiration date. The X.509 standards for certificate content require that digital certificates contain the distinguished (i.e., unique) name of the certificate issuer (the signer), an issuer-specific serial number, the issuer's signature algorithm identifier, and a validity period. The more limited the life of a certificate, the lower the risk exposure for the issuing CA. A certificate's security has both physical and logical vulnerabilities that are outgrowths of the software used to generate a digital signature. The longer such software is in use, the greater the likelihood that it will be corrupted or that someone will gain unauthorized access.

Certificate extensions provide information in addition to the identity of the subscriber and the issuing CA. Additional information may include suggested limitations on uses of the certificate, such as the number of and type of transactions or messages that subscribers are authorized to sign. Any such limitation reduces the transaction and reputation risk of the issuing CA. The CA also may use extensions to establish classes of digital certificates for use with financial transactions or for transmitting highly sensitive information. Such certificates may be for a single

[1] Portions of this discussion were derived from "Certification Authority Systems", Office of the Comptroller of the Currency, OCC 99-20, May 4, 1999.

message or transaction, used only with a specific relying party, or limited to a maximum financial amount.

4.3 Certificate Creation, Distribution, and Acceptance

The process of creating, distributing, and documenting acceptance of a subscriber's certificate exposes a CA to transaction, strategic, and reputation risk. In certificate creation, the transaction and reputation risk exposures arise from possible errors occurring in the systems that match appropriate certificate limitations to each subscriber's unique signing capabilities. Risk exposures are associated with the policies and procedures that control the process.

Certificate distribution and acceptance often are not solely the responsibility of the CA. The subscriber likely will obtain the technology to create digital signatures from a software provider or other technology firm. However, the certificate is not complete until the CA acknowledges the subscriber's signing capability with its own digital signature to create the certificate of record. In a closed CA system, the CA risk exposure may be modified by the contract establishing the exact roles and responsibilities of the parties. Some of the transaction risk may be allocated to a lead organization, individual subscribers and relying parties, or another entity maintaining the database of certificates. However, the CA still may have a reputation risk exposure if problems with the technology are attributed to the CA.

Generally, a digital certificate will not be operational until the subscriber accepts the signed certificate. Certificate acceptance implies that the subscriber agrees to the terms and conditions established by the CA for the overall system as well as any specific conditions that apply to the subscriber. Errors in the communication process with subscribers regarding acceptance, from either inadequate policies and procedures or technical difficulties, expose the CA to both transaction and reputation risk.

4.4 Managing Digital Certificates

When a CA issues certificates to support subscribers' digital signatures, the CA usually is interacting only with subscribers or a representative or agent acting on behalf of the subscribers. However, if the CA also chooses to manage outstanding certificates, i.e., act as a repository, the CA will transact with relying parties that receive messages. The following discussion outlines the risk exposures that arise with respect to repository services for both subscribers and relying parties. It is organized to address four aspects of managing digital certificates:

- Customer disclosures
- Subscriber service and support;
- Suspending and revoking certificates; and
- Processing the requests of relying parties.

4.4.1 Customer Disclosures

Although there is no legal disclosure requirement at present, a CA will need to provide some information concerning the basic services provided and the rights and responsibilities of subscribers and relying parties. The nature of the disclosures will have an impact both on the transaction and reputation risk exposure of a CA. For example, if disclosures clearly describe the CA error resolution procedures and privacy policy, there may be less confusion on the part of subscribers. Further, if the CA provides technical documentation on the use of the software associated with certificates, subscribers will be better able to distinguish between problems resulting from the software rather than the CA, shifting some of the reputation risk exposure away from the CA.

4.4.2 Subscriber Service and Support

Like many new information technology products and services, a CA requires customer support, which is a source of reputation risk. A CA may consider establishing a help desk or some other form of direct interaction with subscribers and relying parties. The policies, procedures and operation of the help desk are a potential source of transaction and strategic risk. Resolving problems or errors that subscribers and relying parties encounter from lack of familiarity with the use of the underlying technology will require substantial resources from the CA or a customer service contractor. Although the CA typically will not supply software for creating a digital signature, there may be some circumstances in which subscribers attribute all difficulties in using the technology to the CA.

Subscribers may have technical problems because of software configurations on their personal computer systems that may not become apparent until they attempt to sign a message or transaction. Because an organization providing CA services ultimately may wish to maintain the customer relationship, the practical decision may be to provide customer service either internally or to contract with a firm with appropriate expertise. Some technology firms now provide smart cards to hold subscriber certificates. Instead of downloading the software to the PC hard drive, the subscriber would have a smart card reader attached to his PC. The smart card and reader would be pre-programmed to load the certificate information appropriately for the subscriber. Some of the transaction and reputation risk of subscriber service and support may be reduced by the simplicity of the use of hardware rather than requiring PC users to load the software from another source.

4.4.3 Suspending and Revoking Certificates

Because the subscriber is responsible for maintaining the security of the signature capability, the potential exists that the system may be compromised and made available for unauthorized use. Thus, the CA may be required to suspend or revoke a certificate. If the CA (or another responsible party within the system) does not monitor and take such action in a timely manner, the CA may authenticate messages or transactions carrying expired digital signatures. Thus, CA systems that render a subscriber's digital certificate invalid are potentially exposed to substantial transaction, strategic, and reputation risks. Poorly designed policies and procedures are a source of strategic risk, and improperly implemented ones expose the CA to transaction and reputation risk. The timing of necessary repository updates may differ with the type of certificates involved; a delay in the suspension of a certificate used for sensitive messages or transactions carries relatively high risk.

A digital certificate may be rendered invalid in one of two ways. The CA may revoke a certificate if it is certain that a subscriber has compromised his signing capability. The most likely compromise would be if the subscriber did not keep his private key secure. If a subscriber's private key became known, unauthorized individuals could sign messages and transactions. If there is some question as to the status of the certificate, the CA instead may suspend the certificate until its status is determined. Transaction and reputation risk may result from errors in processing both requests for revocation and suspension of certificates. For example, a subscriber whose certificate is erroneously invalidated and hence is unable to sign messages could potentially experience losses and may pursue legal action, damaging the CA's reputation in the process. Conversely, the CA may suffer exposure if a relying party accepts a message or transaction that is signed by a subscriber whose certificate should have been revoked or suspended.

4.4.4 Processing Relying Party Requests

Substantial transaction, strategic, and reputation risk exposure is associated with processing requests by relying parties regarding the status of individual certificates. Although the CA-subscriber contractual relationship may define obligations to subscribers and others, such contracted protection may not exist for transactions with relying parties, particularly in open systems. For example, if the CA represents a revoked certificate as operational to a relying party, the CA may be exposed to reputation damage or a lawsuit. There is an additional risk in an open system that the circumstances of an individual subscriber or class of subscribers have changed during the valid period of a circulating certificate. Any delays in processing certificate revocation requests as a result of inadequate policies and procedures or technical processing may result in such errors. If the repository processes requests in batch mode as opposed to real time, the risk exposure is greater. As the volume of transactions processed by the repository increases and as more certificates are placed in circulation with varying limitations and expiration dates, risk exposures also may increase.

4.4.5 Certificate Revocation

There are two recognized methods for responding to a request about the validity of an individual certificate. The most well known method requires the repository to retrieve a lengthy list of invalid certificates, the Certificate Revocation List (CRL), to check the validity of a single certificate. Inaccuracies in the CRL are a source of transaction risk for the CA system. In addition, the scheduled frequency for generating the CRL will affect the risk exposure of the repository. More frequent generation of CRLs will reduce a CA's transaction and reputation risk exposure. There is also an issue as to whether certificate status is "pushed" out by the CA repository to interested relying parties, or "pulled" from the repository by the relying parties in question.

There are different transaction and reputation risk exposures associated with each method. The "pull" method allows the CA repository to transfer any reputation risk exposure successfully to the relying party with respect to accepting an invalid certificate. On the other hand, the "push" method places the responsibility clearly on the CA if the CRL is not accurate or is not distributed on a timely basis. Because of the risks and cost inefficiencies of the CRL approach, the industry is developing a second method. Several technology firms have developed software that allows a repository to search its records for the validity of a single certificate in real time. Another source of repository transaction risk relates to the ability of a relying party to understand certificate extensions.

5 THE FEDERAL PKI

5.1 FEDERAL PKI ARCHITECTURE

Many Federal agencies have initiated efforts to set up independent CAs to support applications such as purchasing, grants, travel, or other functions that are needed to support the agency mission. For these applications, the use of public key technology must be justified in terms of its direct benefit to a specific agency application. Another option is for the agency to use commercial CA service providers to issue certificates and facilitate delivery of services. Agency projects would then pay the commercial CA service provider.

The main issue for the Federal PKI is how to create certification paths between Federal agencies that will provide for reliable and broad propagation of trust. A Bridge CA (BCA) provides systematic certification paths between CAs in agencies, and outside the government. Federal CAs that meet certain standards and requirements will be eligible to cross-certify with the FBCA, thereby gaining the certification paths needed to establish interoperation between the Federal and commercial PKIs. Figure 4 illustrates how bridge CAs will provide interoperability between Federal and other PKIs.

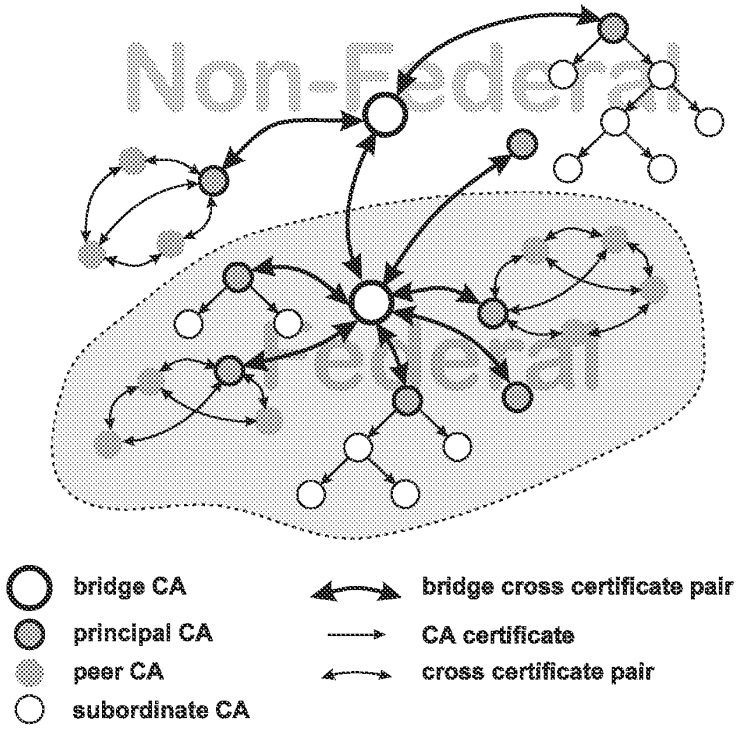


Figure 4. Interoperation Between Federal and Non-Federal PKIs

The Federal BCA will be the unifying element to link otherwise unconnected agency CAs into a systematic overall Federal PKI. It is important to note that the BCA is not a root CA, but is a "bridge of trust". It does not begin certification paths, but connects trust domains through cross certificates between the FBCA and designated principal CAs. A federal policy management authority (FPMA) will supervise FBCA operation and establish the requirements for cross

certifying with the FBCA. These trust domains may be within the government or outside the government.

Federal (or non-federal) CAs that operate in trust domains that meet the requirements established by the FPMA will be eligible to cross certify with the FBCA. The FBCA will then connect them to the overall trust network of the Federal PKI. This will provide relying parties and certificate holders (in their trust domains) with connectivity to the larger Federal PKI. This will be simpler and more effective than trying to manage an ad hoc collection of many cross certifications with CAs in other trust domains.

To provide maximum flexibility to Federal agencies and not intrude upon their prerogatives, agencies will not be required to adopt the FBCA's policies. Rather, agencies will retain the option to use other policies defined by their own internal PMAs, or by commercial certificate service providers. Agencies will not be required to use the FBCA to interoperate with other Federal agencies or organizations outside the Federal government. Alternatively, Federal agencies may communicate directly with an agency/organization to establish requirements for interoperating. Components of the Federal PKI architecture are:

Federal Policy Management Authority (FPMA): this management authority sets the overall policies of the Federal PKI and approves the policies and procedures of trust domains within the Federal PKI. It operates a Federal Bridge CA, and a repository.

Trust Domains: In the Federal context, a trust domain is a portion of the Federal PKI that operates under the management of a single policy management authority. One or more CAs exist within each trust domain. Each trust domain has a single principal CA, but may have many other CAs. Each trust domain has a domain repository.

Domain Policy Management Authority (DPMA): a policy management authority approves the certification practice statements of the CAs within a trust domain and monitors their operation. The DPMAs operate or supervise a domain repository.

Federal Bridge CA (FBCA): The Federal Bridge CA is operated by the FPMA. Its purpose is to be a bridge of trust that provides trust paths between the various trust domains of the Federal PKI, as well as between the Federal PKI and non-Federal trust domains. FPMA- approved trust domains designate a principal CA that is eligible to cross-certify with the Federal FBCA. The FBCA is not a root CA because it does not typically begin certification paths.

Principal CA: A CA within a trust domain that cross-certifies with the Federal BCA. Each trust domain has one principal CA. In a domain with hierarchical certification paths, it will be the root CA of the domain. In a mesh-organized domain, the principal CA may be any CA in the domain. However it will typically be one operated by or associated with the DPMA.

Peer CA: A CA in a mesh domain, a peer CA has a self-signed certificate that is distributed to its certificate holders and used by them to initiate certification paths. Peer CAs cross-certify with other CAs in their trust domain.

Root CA: In a hierarchical trust domain, the root CA is the CA that initiates all trust paths. Certificate holders and relying parties are given the self-signed root CA certificate by some authenticated means and all trust paths are initiated from that point. For hierarchical trust domains, the root CA is also the principle CA for that domain.

Subordinate CA: A CA in a hierarchical domain that does not begin trust paths. Trust initiates from some root CA. In a hierarchical trust domain, a subordinate CA receives a certificate from its superior CA. A subordinate CA may have subordinate CAs of its own to which it issues certificates.

5.2 Federal Certificate Profile(s)

In the interest of establishing commonality and interoperability with PKI communities outside the Federal government, it was decided that the FPKI profile should be based on a "standard PKI profile" but still contain the unique parameter settings for Federal systems[2]. The only widely accepted PKI profile currently on track to become a standard is the Internet Engineering Task Force (IETF) Public Key Infrastructure (PKIX) profile (RFC 2459) developed by the PKIX working group. The profile can be found at http://www.ietf.org/rfc/rfc2459. The PKIX profile, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, identifies the format and semantics of certificates and CRLs for the Internet PKI. Procedures are described for processing and validating certification paths in the Internet environment. Encoding rules are provided for cryptographic algorithms and all fields are profiled in both the version 3 X.509 and version 2 CRL.

The FPKI profile complements the current PKIX profile and stipulates any differences between the two. If an organization needs to implement a subset of the FPKI-compliant certificate and/or CRL, the organization should tailor its X.509 certificate and/or CRL using the parameters stipulated in the Federal PKI together with the parameters stipulated in PKIX. Parameters stipulated in the Federal PKI document should take precedence. An organization deciding to tailor its FPKI-compliant X.509 certificate and/or CRLs to meet its specific needs must document the intended subset profile (referencing FPKI profile as a basis) so that the certificate generation element will know how to populate the program-specific certificates [Fed PKI profile].

The federal certificate Profile describes the contents of five classes of X.509 certificates: end entity digital signature certificates; end entity key management certificates; CA certificates, Bridge CA certificates, and self-signed CA certificates.

- End entity digital signature certificates contain a public key that is designated for validation of digital signatures on objects other than certificates and CRLs.
- End entity key management certificates contain a public key that is designated for key transport.
- CA certificates are any certificates issued by an agency CA to another CA.
- Bridge CA certificates are issued by the federal Bridge CA to agency principal CAs.
- Self-signed CA certificates are generated by CAs for secure distribution to their subscribers.

The following table identifies mandatory and optional extensions for each class of certificate. Further details are contained in the profile; agencies should obtain a copy of the current profile, as well as RFC 2459, before deploying their PKI.

[2] Portions of this discussion were derived from the Federal Certificate Profile, http://csrc.nist.gov/pki/twg.

Certificate extension	Mandatory or Optional	Contents
Key usage	Appears in all certificates	Specifies the set of generic uses for this key. For users or systems, the key may be used for digital signatures on documents, authentication, key management, or data encipherment. For CAs, the keys may be used for verifying signatures on certificates or CRLs.
Basic constraints	Appears in all CA certificates	Indicates the subject is a CA. May define the maximum number of additional certificates in a path. This is used to limit trust to end entity certificate issued by the subject.
Authority key identifier	Appears in all certificates	SHA-1 hash of the public key which verifies the signature on the certificate; used to select the right key
Subject key identifier	Appears in all CA certificates. May optionally appear in end entity certificates.	SHA-1 hash of this public key; this matches the authority key identifier in certificates and CRLs issued by the subject.
Subject alternative name	Optional, but commonly used.	Used to specify a user's email address, or the DNS name or IP address of an Internet host. This information supports the S/MIME application and IPsec protocols, respectively.
Certificate policies	Appears in all certificates	In an end entity certificate, the policies listed describe the level of trust in this certificate. In a CA certificate, this list describes the range of policies for which its certificates may be trusted.
Policy mapping	Appears only in CA certificates. Appears only when the issuer and subject issue certificates under different policies.	Describes which of the subject CA's policies correspond to the issuer's local policies.
Name constraints	Appears optionally in CA certificates.	Used to limit the set of trusted certificates by name.
Policy constraints	Appears optionally in CA certificates.	Used to impose policy requirements and/or prohibit policy mapping.
CRL distribution points	Optional. Appears in all certificates whose revocation status is distributed by indirect CRLs or segmented CRLs.	Used to identify the CRL that covers this particular certificate.

Certificate extensions in the federal PKI

5.3 FEDERAL CRL PROFILE(S)

The Federal PKI Profile specifies two CRL profiles - one for the FBCA, and a second for all other CAs in the Federal PKI. Both profiles are based on the X.509 Version 2 CRL. The version 2 CRL may include two different types of extensions.

The first type is the CRL entry extension, which provides additional information about a particular revoked certificate. The CRL entry extensions identified in the CRL profiles are the certificate issuer and reason code extensions. By default, all of the certificates listed on a CRL were issued by the CA that generated the CRL. If this is not true, the CRL will use the certificate issuer to identify the CA that issued the certificate. The reason code extension describes the circumstances for revocation. A relying party may accept a certificate that has been "superseded," but reject a certificate that was revoked because of "key compromise."

The second type is the CRL extension, which provides additional information about the entire CRL. The CRL extensions identified by the federal profile are authority key identifier, issuer alternative name, CRL number, and issuing distribution point.

The following tables identify mandatory and optional extensions for each class of CRLs. As noted above, further details are contained in the profile. Agencies should obtain a copy of the current profile, as well as RFC 2459, before deploying their PKI.

CRL Extension	Mandatory or Optional	Contents
CRL number	Appears in all CRLs	Monotonically increasing integer; may be used to detect emergency CRL generation
Authority key identifier	Appears in all CRLs	SHA-1 hash of the public key which verifies the signature on the CRL; used to select the right key
Issuer alternative name	optional	Can be used to specify the CA's email address
Issuing distribution point	Appears in all indirect and segmented CRLs	Contents must match the CRL distribution points extension in the certificates covered by the CRL

CRL Extensions in the Federal PKI

CRL entry extension	Mandatory or Optional	Contents
Reason code	Appears for every certificate, unless the CA has no information	Specifies if the certificate was revoked because the key were compromised, the subject's affiliation changed, or it was superseded by a newer certificate.
Certificate issuer	Appears in all indirect CRLs	Identifies the issuer for a subset of the certificates listed in this CRL.

CRL Entry Extensions in the Federal PKI

6 DEPLOYING AN AGENCY PKI

Agency PKIs will, in most cases, be developed in some degree of isolation. The PKI will be developed to meet internal requirements, where both the subscriber and the relying party are users within that agency. As the agency's confidence and experience increases, it may become cost effective to integrate the agency PKI into the Federal PKI. Adequate planning can ensure that an agency PKI is ready to join the broader Federal PKI, providing access to security services with a growing community of users. This section recommends steps for setting up an agency PKI.

There are numerous impediments and challenges in creating an agency PKI that will interoperate with other federal PKI's. Therefore, it is important to as much as possible follow existing standards and coordinate with the Federal PKI Steering Committee (FPKISC). Some of the challenges an agency will face include the significant cost that can be associated with implementing a PKI, including the cost of creating and distributing certificates, purchasing or creating client software, and in maintaining and supporting users of the PKI. As well, different vendors may implement standards differently, and therefore interoperation of directories and other associated software between PKI's will be tricky.

Accordingly, NIST recommends that agencies follow the steps in this chapter when deploying an agency PKI or PKI pilot. In particular, NIST recommends following the FBCA policy and adhering to the federal certificate profile and CRL extensions profile. It would be best if agencies assume that at some point their PKI will cross-certify with the federal bridge CA, therefore coordinating the development of an agency PKI with the FPKISC is highly recommended. The following sections contain information and steps for developing an agency PKI such that interoperability problems will be minimized.

6.1 ANALYZE DATA AND APPLICATIONS FOR YOUR ORGANIZATION

Installing a PKI can have a significant impact on the security model of an information technology operation. As with most security planning, the agency PKI must be designed using the familiar principles of Risk Management. Planning should begin with risk analysis. In addition to comparing the initial and operating costs of the PKI with anticipated cost-reductions, the cost-benefit analysis should attempt to identify larger risks from not implementing a PKI.

The next step is to identify the data and applications that need to be secured within the agency's computing system. Data may include data used during execution, stored data on magnetic media, printed data, archival data, update logs, audit records, and documentation. Applications may include local/network communications, access controls, and Internet applications. The analysis should also determine the impact if security is compromised, and the degree of risk will determine the appropriate level of assurance for the agency PKI. For example, the more limited the life of a certificate, the lower the risk exposure for the issuing CA. More than one policy may be required if there is a wide variation of risk associated with different applications.

Record retention is always a concern for government agencies, and the movement toward paperless operations will result in significant changes in long-term storage of records. The National Archives and Records Administration (NARA) has developed guidance on records management for agencies implementing electronic signature technologies [NARA00]. The NARA guidance should be consulted during the planning phase to ensure proper record retention practices.

6.2 Collect Sample Policies and Base Standards

It is efficient to begin the development of the PKI by collecting sample policies and using them as templates to develop the agency's own policy(s). Collections of standards are also required for writing your policy(s) because standards are the basis for achieving interoperability between agencies. The following is a list the standards and their references.

FBCA policy FBCA policy is used for determining which level(s) are consistent with the agency's requirements. Current FBCA policy can be found in http://csrc.nist.gov/pki/twg/y2000/doc_reg_00.htm – Bridge Certification Authorities. Final policy will be posted at http://csrc.nist.gov/csor.

- **FPKI X.509** Certificate and CRL Extensions Profile. As part of FBCA policy, this document specifies the version 3 (v3) X.509 certificate and version 2 (v2) Certificate Revocation List (CRL) profiles for Federal Public Key Infrastructure (FRKI) systems. The profiles serve to identify unique parameter settings for FPKI. The Federal certificate profile is located at http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls —Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile.

- **X.500 directories** The certificates or other digitally signed instruments issued by the FBCA and, where applicable, agency CAs, will reside in the FBCA X.500 directory. Directory references are listed at http://csrc.nist.gov/pki/twg/directory_references.htm.

6.3 Draft Certificate Policy(s)

The first requirement for an agency developing a PKI is to establish appropriate certificate policy(s) (CP). The policy(s) must reflect the types of applications that will be secured by the PKI. An effective strategy is to adapt and reuse existing policies (especially FBCA) to create policy(s) for the agency. Certificate policies should be at a sufficiently high level that the policies will not change too frequently. The format and content of these policies is discussed in further detail in section 6.3.1.

The set of policies under which a CA issues certificates is termed its **trust domain** or **policy domain**. The agency needs to obtain an object identifier (OID) for each of the policies in its *trust domain*. These OIDs will be used to differentiate the appropriate set of applications for a particular certificate. An X.509 v3 certificate may state one or more certificate policies in the **certificatePolicy** extension. A **certificatePolicy** extension contains one or more **policyIdentifiers**. A **policyIdentifier** is a unique, registered OID that represents a certificate policy in a certificate. Applications may use these policies to decide whether or not to trust a certificate for a particular purpose. The registration process follows the procedures specified in ISO/IEC, (i.e., joint International Organization for Standardization and International Electrotechnical Commission), and International Telecommunications Union (ITU) standards. The application that registers the OID also needs a textual specification of the certificate policy, for examination by certificate users and other applications. If an agency issues under a single policy, it should still obtain an OID for that policy. When the CA joins the federal PKI, it will be used to differentiate its certificates from the many policies used in the federal government. Procedures to obtain an OID will be covered in section 6.3.2.

6.3.1 Certificate Policies

Policies are generally written in standard format. RFC 2527, the Certificate Policy and Certification Practices Framework, defines the accepted standard CP format. RFC 2527 includes a standard outline with eight major sections and 185 second and third level subsections. Most CPs are written to this outline, since the standard format has a number of distinct advantages. The FBCA CP is consistent with RFC 2527.

By adhering to a well-defined format, the CP writer is less likely to forget something important. It would be easy to overlook a few of the 185 topics identified in RFC 2527 if the author changed the outline. Adhering to the standard format will also simplify cross-certification with other CAs. The cross-certification process should always include a comparison of the other CA's certificate policies. This information is used to determine the contents of the policy mappings and policy constraints extensions to be included in the CA certificates. The eight major sections are summarized below; for details the reader should obtain RFC 2527.

- The **INTRODUCTION** explains how to identify certificates issued under this policy (i.e., the OID that will appear in the policy extension), defines the community for these certificates (e.g., NIST employees, or financial managers,) and provides contact information for the people who administer the CA and maintain the policy.
- The **GENERAL PROVISIONS** captures broadly applicable legal and general practices information. For example, this section identifies the various participants in the PKI (e.g., CA, RAs, subscriber, and relying party) and their various obligations and liabilities. It identifies the applicable laws, fees, and auditing requirements. This section also describes what information (if any) will be considered confidential and the circumstances that would justify disclosure (e.g., a subpoena.).
- **IDENTIFICATION AND AUTHENTICATION** describes the procedures used to authenticate requests for certificates, or for certificate revocation.
- **OPERATIONAL REQUIREMENTS** describes the operations that must be performed by the CA, RAs, end entities, or other parties under this policy. Specific actions are identified that must be performed when requesting or generating new certificates, revoking certificates, creating and protecting audit logs, archiving records, changing the CA's key, disaster recovery, and terminating the CA's operations.
- **PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS** describes how the PKI uses physical security (e.g., guards, guns, and gates), procedures (e.g., separation of duty), and personnel requirements (e.g., background checks and procedures) to complement the technical security controls.
- **TECHNICAL SECURITY CONTROLS** describes the security measures used to protect cryptographic keys (e.g., a FIPS 140-1 validated hardware module), protect critical security parameters (such as the list of trusted RAs), and provide quality assurance for the systems (e.g., a NIAP evaluation), and protect the CA from network-based attacks.
- **CERTIFICATE AND CRL PROFILES** specifies the certificate and CRL profile. This section specifies the cryptographic algorithms that will be used to sign the certificates, the length of the signing key, and the name forms that will appear in certificates. It describes the extensions that are included in certificates and CRLs. For federal agencies, this should correspond closely to the federal profile discussed above.
- **SPECIFICATION ADMINISTRATION** is the final section, and it describes how the policy will be maintained. It describes the procedures that will be followed if the specification is changed, how those modifications will be published, and the approval procedures.

CP authors should not develop their documents in a vacuum. CP authors should search the available CPs and identify CPs with similar scope and requirements. These CPs should be used as inputs to the CP development process. Example Certificate Policies are available from a number of sources, including U.S. Federal CPs that may be found at http://csrc.nist.gov/csor/pkireg.htm.

6.3.2 Computer Security Objects Registry

As noted above, government agencies should include an appropriate policy OID in all certificates that it issues. NIST maintains the Computer Security Objects Register (CSOR), one of the CSOR's functions is the assignment of object identifiers for PKI certificate policies.

The CSOR has allocated the following registration branch for Public Key Infrastructure (PKI) objects:

csor-certpolicy={joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1)}.

Government agencies may obtain OIDs in this arc by submitting a RFC 2527-formatted Certificate Policy to csor@nist.gov.

In addition, NIST has defined a set of OIDs that may be used during pilot testing of PKIs. The policies associated with these OIDs have no meaning, but may be used to verify the correct operation of certificate policy mechanisms.

6.3.3 Establishing Policy Mappings and Constraints

As agencies progress from a single isolated CA to more sophisticated architectures, they will establish trust relationships between certification authorities. These relationships are manifested as CA certificates. Where CAs issue certificates under common policies, the contents of these certificates are straightforward. The certificate policy extension contains the OIDs for each of the policies shared by the two CAs. There is no need for policy mapping, or policy constraints.

When two CAs issue certificates in different policy domains, procedures become more complicated. Each CA must review the other CA's policies, and determine which of their own policies (if any) they satisfy. These policy relationships are encoded in the policy mapping extensions. If one of the other CA's policies is deemed entirely unacceptable, a CA may include policy constraints in the CA certificate it issues. This extension permits a CA to specify a limited set of policies that are acceptable. As a result, certificates issued under the unacceptable policy will be rejected.

6.3.4 Local certificate and CRL profile(s)

To maximize interoperability, the local certificate and CRL profile must be consistent with the Federal Certificate and CRL Profile described above. That is, the certificate issued by a federal agency must contain all required fields and extensions. The federal agency may mandate inclusion of optional features and add private extensions. However, the private extensions must never be marked as critical. Certificates with unrecognized critical extensions are ignored, so marking private extensions as critical would limit interoperability.

The following table describes consistency:

	Federal Profile	A Consistent Local Profile
Basic certificate fields	Does not use unique identifiers	Does not use unique identifiers
Standard (ISO or IETF) extensions	Mandatory extensions	Mandatory; must match in criticality
	Optional extensions	Mandatory, optional, or never populated. If present must match criticality setting in federal profile.
	Omitted extensions	Must not be used if critical
Private extensions	None	Must be noncritical

6.4 Select PKI Product or Service Provider

The next step after planning is to select the appropriate PKI product or service provider. The agency needs to review the candidate products or service providers to determine which can implement the agency's policy(s). The following lists aspects to be considered for the selection.

- Compatibility and interoperability with other PKI products/service providers.
- Ease of adoption to open standards.
- Minimum proprietary application program interface (API) dependency.
- Ease of supporting applications such as virtual private networks, access control, secure e-commerce, smartcard management, smartcards and hardware, directories, secure messaging, secure forms, enterprise, and others.
- Ease of deployment.
- Flexibility of administration.
- Scalability and portability of installation.

6.5 Develop CPS (Certification Practice Statement)

After the selection of vendor product or service provider the agency need to develop a highly specific document, a CPS (Certification Practice Statements), that describes how an agency (or service provider) will implement the policy(s) developed in 6.3. A CPS is a statement of the practices that a particular CA employs in issuing certificates. A CPS describes the details of the system used and the practices employed by a CA to issue certificates, and it details the procedures used to implement the policies identified in the certificates issued by a CA, including the means used to identify certificate subjects. The CPS also states the means used to protect the private key of the CA, and the other operational practices followed by the CA to ensure security. Each Federal CA will post its CPS in the BCA Repository, and also post the CPS in any repository associated with the CA. The basic list of topics to be covered is the same for both a certificate policy (CP) and a CPS as stated in Section 6.3.1.

6.6 Do a Pilot

PKIs are non-trivial. It is recommended that the agency start by supporting a limited number of users and use it for internal applications first. During the pilot the following operations need to be exercised:

- Set up test accounts (users) for all application that will use the PKI.
- Test all the administration operations to make sure they all work properly.
- Shut down the system, bring it back up, and check that everything works correctly.
- Test all PKI functions of the applications locally and remotely (through network if applicable).
- Make sure that the agency has the physical security and personnel controls in place to support the PKI.
- Repeat 6.3, 6.4, and 6.5 to incorporate lessons learned.

6.7 Apply for Cross Certification with the FBCA

Once the PKI and critical applications work well internally the agency may choose to cross-certify directly with the agencies it commonly deals with. However, the most efficient mechanism for joining the federal PKI is cross-certification with the FBCA. To join the FBCA, one of the important steps is to establish policy mappings and constraints as described in 6.3.1

If the agency wishes to cross-certify its PKI with the FBCA, the first step is to select a principal CA. If the agency PKI has only one CA, it is the principal CA. If the agency PKI is a hierarchy, the principal CA must be the root CA. If the agency PKI is a mesh, the agency is free to select any of its CAs as the principal CA.

The FBCA Policy Management Authority processes requests to cross-certify with the bridge. While procedures are still being finalized, the FBCA will require an agency to submit its CP(s) and may request an independent audit to ensure the CP is being implemented faithfully. The FBCA will determine a mapping between its four certificate policies, which specify four increasing levels of assurance, and the policies that comprise the agency PKI's trust domain. Once an agency PKI cross-certifies with the FBCA, that agency is given a seat in the FBCA Policy Authority.

7 SUMMARY AND CONCLUSIONS

As Federal agency operations are moved online, information technology security services based on cryptography become essential. Public key cryptography can play an important role in providing needed security services including confidentiality, integrity, authentication, and digital signatures. Public key cryptography uses two electronic keys: a public key and a private key. The public key can be known by anyone while the private key is kept secret by its owner.

Public key cryptography is straightforward to implement for a pair of users and a single application. This technology will scale easily to support a few applications or a small community of users. However, as the community grows, it becomes difficult to distribute the public keys and keep track of the user that owns the corresponding private key. To use public key cryptography on a broad scale, users need the support of a security infrastructure to manage public keys.

A public key infrastructure (PKI) allows public key cryptography to be employed on a broad scale. With a PKI, parties who have not met in person are able to engage in verifiable transactions. The identity of the originator of a message can be traced to the owner of the private key as long as there is strong binding between the owner and the owner's public key. A PKI provides the means to bind public keys to their owners and helps in the reliable distribution of public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable Certification Authority (CA).

A PKI is often composed of many CAs linked by trust paths. The CAs may be linked in several ways. They may be arranged hierarchically under a "root CA" that issues certificates to subordinate CAs. The CAs can also be arranged independently in a network. Recipients of a signed message with no relationship with the CA that issued the certificate for the sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate.

The confidence that can be placed on the binding between a public key and its owner depends much on the confidence that can be placed on the CA that issued the certificate that binds them. Provisions in the X.509 standard enable the identification of policies that indicate the strength of mechanisms used and the do's and don'ts of certificate handling. The rules expressed by certificate policies are reflected in certification practice statements (CPSs) that detail the operational rules and system features of CAs and other PKI components. By examining the policies associated with a sender's certificate, the recipient of a signed or encrypted message can determine whether the binding between the sender and the sender's key is acceptable and thus accept or reject the message. By examining a CA's CPS, users can determine whether to obtain certificates from it, based on their security requirements. Other CAs can also use the CPS to determine if they want to cross-certify with that CA.

This publication may be used to assist Federal agency decision-makers in determining if a PKI is needed by their agency, and how PKI services can be deployed most effectively within an agency. It provides an overview of PKI functions and their applications. Additional documentation will be required to fully analyze the costs and benefits of PKI systems for agency use, and to develop plans for their implementation. This document provides a starting point and references to more comprehensive publications.

8 ACRONYMS AND ABBREVIATIONS

ACES	Access Certificates for Electronic Services
API	Application programming interface
ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECA	External certification authority
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FBCA OA	Federal Bridge Certification Authority Operational Authority
FED-STD	Federal Standard
FIPS PUB	Federal Information Processing Standard Publication
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GITSB	Government Information Technology Services Board
GPEA	Government Paperwork Elimination Act of 1998
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
MOA	Memorandum of Agreement (as used in the context of this CP, between an Agency and the FPKIPA allowing interoperation between the FBCA and Agency Principal CA)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm, Version 1
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

9 GLOSSARY

Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the Federal PKI Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.

Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it's Subscriber, (3) contains the Subscriber's public key, (4) identifies it's operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect.
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate that is composed of two subfields; "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Agency as defined above.
Encrypted Network	A network on which messages are encrypted (e.g. using DES, AES, or other appropriate algorithms) to prevent reading by unauthorized parties.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Agency Principal Certification Authorities.
Federal Bridge Certification Authority Membrane	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.

FBCA Operational Authority	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum	Agreement between the Federal PKI Policy Authority and an Agency allowing

of Agreement (MOA)	interoperability between the Agency Principal CA and the FBCA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the Federal PKI Policy Authority.
Principal CA	The Principal CA is a CA designated by an Agency to interoperate with the FBCA. An Agency may designate multiple Principal CAs to interoperate with the FBCA.
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of

	an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment	A comprehensive accounting of all system hardware and software types and settings.

Configuration	
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

10 SELECTED BIBLIOGRAPHY

[BDNP 98] Burr, W., D. Dodson, N. Nazario, W.T. Polk. *Minimum Interoperability Specification for PKI Components (MISPC), Version 1.* NIST SP 800-15. National Institute of Standards and Technology, January 1998.
http://csrc.nist.gov/publications/nistpubs/800-15/SP800-15.PDF

[CJB 01] Chang, S., Johnson, R., and W. Burr, "Federal PKI Directory Profile", working document, http://csrc.nist.gov/pki/twg/y2001/doc_reg_01.htm.

[COOP 99] Cooper, D.A. "A model of certificate revocation," Proceedings of the Fifteenth Annual Computer Security Applications Conference, pages 256-264, December 1999.

[DH 76] W. Diffie, M.E. Heilman, "New Directions in Cryptography," IEEE Transactions on Information Theory, v. IT-22, n. 6, (Nov 1976), pp. 644-654.

[ENTR 00] Entrust Technologies. "The PKI: Paving the Way for Secure Electronic Service Delivery," January, 2000.

[HCFA 01] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Page, http://www.hcfa.gov/hipaa/hipaahm.htm

[HP 01] Housley, R., and W.T. Polk. *Planning for PKI: Best practices for PKI Deployment,* Wiley & Sons, 2001.

[IETF 99] RFC 2104 HMAC: Keyed-Hashing for Message Authentication.
http://www.ietf.org/rfc/rfc2104.txt

[IETF 01] Public-Key Infrastructure (X.509) (pkix)
http://www.ietf.org/html.charters/pkix-charter.html

[LEE 99] Lee, A. *Guideline for Implementing Cryptography in the Federal Government*, NIST SP 800-21. National Institute of Standards and Technology, November, 1999.
http://csrc.nist.gov/publications/nistpubs/800-21/800-21.pdf

[LYON 00] Lyons-Burke, K. "Federal Agency Use of Public Key Technology for Digital Signatures and Authentication," NIST Special Publication 800-25, October 2000.
http://csrc.nist.gov/publications/nistpubs/800-12/

[MOSE 99] Moses, T. "Trust Management in the Public Key Infrastructure," Entrust Technologies, January 14, 1999. http://www.entrust.com/resources/pdf/trustmodels.pdf

[NARA 00] National Archives and Records Administration, "Records Management Guidance for Agencies Implementing Electronic Signature Technologies", October 18, 2000", http://www.nara.gov/records/policy/gpea.html

[NIST 01] National Institute of Standards and Technology. *Certificate Issuing and Management Components Protection Profile*,
http://csrc.nist.gov/pki/documents/CIMC_PP_final-corrections_20010126.pdf

[NIST 97] National Institute of Standards and Technology. Public Key Infrastructure Technology, ITL Bulletin, July 1997. http://www.nist.gov/itl/lab/bulletns/archives/july97bull.htm

[NIST 94] National Institute of Standards and Technology. FIPS 140-1, *Security Requirements for Cryptographic Modules,* Jan. 1994.
http://csrc.nist.gov/publications/fips/fips1401.htm

[NIST 95] National Institute of Standards and Technology. FIPS 180-1, *Secure Hash Standard*, April 1995. http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf

[NIST 00] National Institute of Standards and Technology. "X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), Version 1.4R, March 4, 2000. http://csrc.nist.gov/pki/fbca/FBCA_CP_20001227.doc

[NIST 01b] "Draft FIPS for the AES", http://csrc.nist.gov/encryption/aes/index.html.

[RSA 78] R.L. Rivest, A. Shamir, L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v. 21, n. 2 (Feb 1978), pp. 120-126.

[TREA 99] Office of the Comptroller of the Currency. "Certification Authority Systems", OCC 99-20, May 4, 1999.

Security Issues for Contactless Smart Cards

Michael W. DAVID[1] and Kouichi SAKURAI[2]*

[1] CUBIC Coproration., International Business Development
111 8th Ave., Suite 700, New York, NY, 10011, U.S.A.
email:mike.david@cubic.com
[2] Kyushu University, Compuer Science Dept.
6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-81, Japan
e-mail: sakurai@csce.kyushu-u.ac.jp

Abstract. We review the current technologies of contactless smart cards and compare them with contact cards. We discuss the problems of implementing encryption in contactless cards, and consider how to solve the problems. We also report the state of standardization of contactless smart card.

Keywords. Public key, Smart-card, Contactless-card, Standards, Efficient Implementation

1 Introduction

Smart cards are important tools for the implementation of public key cryptosystems (PKC). There are some pilot systems in electronic cash (e-cash) for banks. The existing cards implementing PKC are for the most part, still contact cards. However, for application to transit systems like railways and highways, the card shall be non-contact: contactless cards are required.

A technical problem for implementing PKC in Contactless Smart Cards (CSC) is the limitation of the card's power of computation and communication: transactions in less than 100 milliseconds (ms) are desired. Even if we can implement RSA cryptosystem [RSA] over contactless cards, it takes too long to execute the encryption/decryption because RSA requires many arithmetic operations over large modulus. Even the elliptic curve cryptosystems with smaller size keys [Mil,Kob] are still slow, which is 10-times faster than RSA.

So, one direct solution is to develop a new public key algorithm, which is much more efficient than RSA. Another solution is to design a new protocol that reduces the computational tasks of the CSC.

This review reports the current technologies of CSC while comparing them to contact cards. Then we discuss the problem of implementing PKC in the CSC, and discuss how to solve the problem. We also mention the state of standardization of contact/contactless smart-cards.

---

* This work was done while visiting in Columbia Univ., Computer Science Dept. from September 1997 for one year.

2 On Contactless Smart Card (CSC)

2.1 Applications

The applications we have focused on are in public transport. We have considered public transport applications as primarily those found in subway and bus systems, but can include parking lot and taxi revenue collection schemes. These cards are different from those used in toll road collection, since the distance for toll road systems far exceeds the 10 cm transmission distance defined by ISO/IEC 14433343. However, the ISO/IEC 14443 type of card could also be used for access control, ID cards, telephone cards and other areas, depending on the users needs and operating methodology.

2.2 Products (Single frequency)

MIFARE, a registered trademark, was developed by Mikron GmbH. Mikron is now owned by Phillips Semiconductors, and has a major share of the installed contactless smart card base. For example, the Korean firm INTEC, has used the MIFARE card for large scale applications in Korea bus fare collection system. It is also being tested for applications in Korean subways. MIFARE will also be adopted (Single frequency) by the light rail system in Kuala Lumpur and the subway in Shanghai.

Japan's NTT Corporation will be using a CSC for its new telephone card system.

FELICA, a registered trademark, was developed by the Sony Corporation. It is the basis for Hong Kong's "Octopus' card, being used by the Creative Star Limited consortium. Creative Star uses the cards to integrate fare collection on the subway, bus and ferry systems in Hong Kong.

GO CARD, a registered trademark, was developed by the Cubic Corporation. It will be in use in the Chicago and Washington D.C. transit systems. As in Hong Kong, this will apply to multiple modes of transportation to include subway, bus and parking lots.

3 Technical Issues for Cryptographic Applications

3.1 Requirements

Based on experience with the use of existing magnetic fare card systems, and the needs for high passenger throughput, we believe that public transport applications will be a complete transaction speed of less than 100 milliseconds (ms). This includes the need to authenticate, read, write and verify card integrity and values, along with any security related processing. However, transit authorities would like to see these contactless cards migrate in the future to be compatible with the contact cards that will be used by the electronic cash (e-cash) and debit card markets.

3.2 Issues

None of the cards listed in Subsection 2.2 are compatible. Due to variations in modulation, bit coding, protocol, power requirements and approached to security, it is very difficult to configure one reader/writer unit to simultaneously deal with all three products.

Users want to have the ability to combine contact and contactless functions on one card. This is sometimes referred to as a combination or "combi-card". However, the security requirements for an e-cash or debit card are much higher than that of a stored value transit card. In the long term, there may be a move to the expanded use of contactless cards because of the simplicity of the installation of the read/write (r/w) system. However, the fabrication of contactless cards is much more difficult than that of contact cards. The difficulty lies primarily in the placement of the wire leads to the chip contact plates. If this process fails or if the placement of the wires are not secure, the contactless card will not function.

3.3 Market Movements

There are a few approaches that are being taken to deal with the issue in the previous.

The first is to develop a contactless ASIC and a micro-controller to a common memory module, permitting a one chip solution. The shared memory case has the advantage that the value or purse can be loaded through the more secure contact interface. However, this still lacks the ability to permit contactless debits of bank products such as Mondex or Visa Cash due to the inability to exercise the micro-controller based security functions without contact. There are products like this being developed. One uses a Siemens micro-controller and a MIFARE ASIC. Another will use a Motorola microprocessor and a Sony FELICA-based ASIC. Motorola is working on its own contactless micro-controller for integration with the PROTON e-cash system.

The second is to develop a two-chip hybrid card with both a contactless ASIC and a micro-controller, each with its own dedicated memory. This alternative is similar functionally to the one chip solution, but does not enable loading value to the contactless portion from a contact terminal. The advantage is that because the chips are separate, there is no security threat to the contact e-cash / banking side of the card.

Although more difficult from the security perspective, the market may drive a solution based on the one-chip, common memory combi-card.

4 Towards Cryptographic Solutions

How to provide e-cash/debit card level security for the combi-card that permits contactless transactions in less than 100 ms.

4.1 Developing a new very efficient PKC

Even if we can implement RSA cryptosystem over contactless cards, it takes too long to execute the encryption/description because RSA requires many arithmetic operations over large modulus (e.g. 2048 bits). Even the elliptic curve cryptosystems with smaller size keys are still slow, which is 10-times faster than RSA.

So, one direct solution is to develop a new public key algorithm, which is more efficient than RSA. Such an attempt was initiated by Matsumoto and Imai [MI], and modified by Patarian [PG], which use multivariate polynomials and would achieve speeds 100 times faster than RSA.

4.2 Developing a new protocol

Another solution for implementing PKC over contactless cards, instead of developing a new encryption algorithm, is to design a new protocol that decreases the computation tasks of the CSC. In protocols which add a powerful server[MILY], indeed the computation task of cards decreases, however, the number of interactions between the server and cards increases, or the required communication data increases.

A new scheme of signcryption developed by Zheng[ZHE] is a possible solution to this problem. This scheme needs only a few rounds of communication, and less data to be sent based on the current public key algorithms.

5 Standarization

5.1 Contact card

Conventional contact smart cards center around the market for identification (ID) cards, bank cards and telephone cards. The key standards associated with these type of cards are International Standards Organization (ISO) 7810 - 7816. These standards focus on card attributes such as dimension, material quality, magnetic strips placement, embossing standards, integrated circuit (IC) chip placement and interfaces. They are widely accepted throughout the banking and telephone card industries.

There is also a market driven form of standard being adopted by Europay, MasterCard and Visa. This is referred to as the EMV. These uses the physical card standards prescribed by ISO 7810 - 7816. However, the EMV expands the standardization effort to cover smart card initialization, security, operating system utilization and application development and activation issues.

There are also other industry associations working toward commonality within the contact card market.

The Multiple Operating System (MULTOS) [multos] initiative designed to permit multiple stored value e-cash systems on one chip. For example, the use of Mondex, Proton or VisaCash on one card. The OpenCard Framework (OCF)

was announced in March 1997, and is an open standard that provides for interoperability of smart applications across many platforms to include network and personal computers, ATMs, GSM/PCS cellular phones

The Global Chipcard Alliance (GCA) established in November 1997 designed to address interoperability of primarily telephone card systems. However, its goal is to permit multi-functional smart card technology.

5.2 Contactless card

The ISO/IEC 14443 is an initiative underway to define a proposed standard for contactless or proximity cards. It relates to cards that would be used within a read distance of 10 cm or less. The topics under evaluation are:

Part-I : Physical Characteristics
Part-II : RF Power and Signal Interface
Part-III: Initialization and Anti-Collision
Part-IV: Transmission and Protocols

As of the fall of 1997, there was agreement on Part-I. This is true due to the close association with existing ISO 7810 - 7816.

Part-II involves some of the following key elements: (1) Frequency of data transmission, (2) Data rate, (3) Modulation, and (4) Bit coding.

There is basic agreement on the use of the frequency of 13.56 megahertz (mhz) for power, read and write functions. Modulation and bit coding at this point in time differ according to various card applications designers. Some form of standard to provide interoperability between different contactless and reader-writer (r/w) equipment may be necessary to permit users to use multiple suppliers. However, there is as yet no agreement in this area.

Part-III relates to data content for sign-on and sign-off functions. This basically allows the card and its target (r/w) unit to ensure that a transaction has been completed. This is very important in the contactless environment. The contact card is captures and read inside a controlled r/w environment (e.g. inside an ATM or a public telephone). However, the contactless card must operate at the whim of the users hand and arm movements, as well as the surrounding electro-magnetic environment. At this point in time, different methods to deal with these issues.

Part-IV deals with transmission, protocols and security. These are important issues, but are far from being defined within the ISO/IEC 14443 initiative.

6 Concluding Remarks

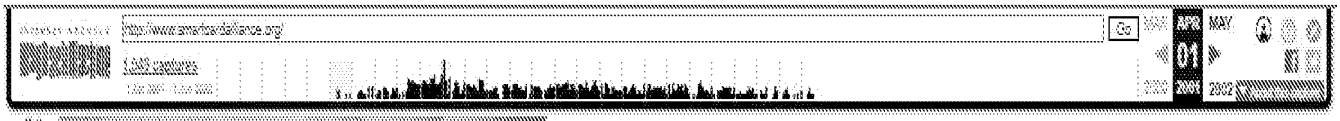
This paper has reviewed the current technology of contactless cards with a smart chip, and reported the standardization efforts for this technology. Then we considered the difficulty and possibility of public-key crypto's being implemented in Contactless Smart Cards, and discussed future cryptographic topics to be developed for the implementation of PKC over Contactless Smart Card.

Acknowledgments

The authors would like to thank Tohru Inoue of Advanced Mobile Telecomm. Security Tech. Research Lab. for his support on this work. The second author wishes to thank Zvi Galil and Moti Yung for their hospitality while visiting Columbia Univ. Computer Science Dept. Final thanks to Hideki Imai and Yuliang Zheng for giving the first author a chance to present this survey at PKC'98.

References

[Amm] http://www.ammismartcards.com
[Car] http://www.cardshow.com Smart Cards and Systems: Vol 2, Issues 30, 35, 36, 40
[Cer] http://www.certicom.com
[Gem] http://www.gemplus.com
[GUQ] L.C.Guillou, M.Ugon, and J.-J. Quisqater "The smart card: A standardized security device dedicated to public cryptology," in Contemporary Cryptography, edited by G.J.Simmons, IEEE Press.
[Kob] N.Koblitz, "Elliptic Curve Cryptosystems," Math.Comp. Vol.48 (1987).
[Mil] V.S.Miller, "Use of Elliptic CURVES in Cryptography," Proc. CRYPTO'95.
[MI] T.Matsumoto and H.Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption" Proc. Eurocrypt88.
[MILY] T.Matsumoto, H.Imai, C.S. Laih and S.M.Yen, "On verifiable implicit asking protocols for RSA computation," Proc. ASIACRYPT'92.
[Mul] The Web site at http://www.multos.com
[PG] J.Patarin and L.Goubin, "Trapddor one-way permutations and multivariate polynomials," in Proc. ICICS97.
[Ram] http://www.ramtron.com
[RSA] R.Rivest, A.Shamir, and L.Adleman, "A method for obtaining digital signatures and public key cryptosystems," CACM 21 (1978).
[Slb] http://www.slb.com/ms/et
[Zhe] Y. Zheng, "Signcryption and its applications in efficient public key solutions," in Proc. Information Security Workshop'97.



Smart Card Alliance

The Alliance

Welcome to the Smart Card Alliance, the combination of the two leading US smart card organizations, the Smart Card Forum and Smart Card Industry Association.

Memberships Approve Creation of the Smart Card Alliance

New York, New York January 22, 2001 – The Smart Card Industry Association (SCIA) and the Smart Card Forum (SCF) announced today that their members have unanimously agreed to combine the two organizations to form the Smart Card Alliance (the Alliance). The Alliance will be the largest smart card oriented, non-profit entity in the world with over 225 member organizations, and will serve as a single voice for the smart card industry in the United States. Complete Text

Alliance Press Releases

Learn About Smart Card Technology Applications

Learn about Smart Card technology, history, applications, standards, specifications, security, reliability, books, news, industry resources and more.

Knowledge Base

Post in the SCA Discussion Forum

Post questions to industry experts in the discussion forum. This discussion forum has been hosted by SCIA and contains information on many topics not covered in the Knowledge Base.

Discussions

Industry Shaping Events

Track the industry's significant events. Updated monthly, this section summarizes the daily news into events which shape the industry.

Happenings

Copyright © 2001 Smart Card Alliance, Inc. All rights reserved. The material in this presentation may be distributed and copied for personal and non-commercial purposes only. Redistribution and reproduction, including posting on news groups, is expressly prohibited without prior written consent.

We welcome comments and suggestions. Please email to Smart Card Alliance

PTO/SB/81C (12-08)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REEXAMINATION - THIRD PARTY REQUESTER POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Control Number(s)	
Filing Date(s)	October 23, 2014
First Named Inventor	John J. Giobbi
Title	Biometric personal data key (PDK) authentication
Patent Number	US 9,298,905
Examiner Name	
Attorney Docket No(s).	02198-00080

I hereby revoke all previous requester powers of attorney given in the above-identified reexamination proceeding control number(s).

☐ A Power of Attorney is submitted herewith.

OR

☐ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

OR

☒ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number
Marissa Ducca	59807
James M. Glass	46729

Please recognize or change the correspondence address for the above-identified reexamination proceeding control number(s) (more than one may be changed **only** if they are merged proceedings) to be:

☐ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☒ Firm or Individual Name	QUINN EMANUEL URQUHART & SULLIVAN LLP c/o Marissa Ducca				
Address	1300 I Street NW, Suite 900				
City	Washington, D.C.	State	Washington, D.C.	Zip	20005
Country	US				
Telephone	(202) 583 8000	Email	marissaducca@quinnemanuel.com		

I am the *third party* requester.

☒ Proof of authority to act on behalf of requester submitted herewith or filed on _____ .

SIGNATURE of Third Party Requester

Signature	/s/ Brittany McElmury Dietz	Date	6/8/2022
Name	Brittany McElmury Dietz	Telephone	
Title and Company	Senior Legal Counsel Samsung Electronics America, Inc.		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



Contactless Payment and the Retail Point of Sale: Applications, Technologies and Transaction Models

A Smart Card Alliance Report

Publication Date: March 2003

Publication Number: PT-03002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 1-800-556-6828

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, health care, retail and entertainment industries, as well as a number of government agencies. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. For more information, visit www.smartcardalliance.org.

Copyright © 2003 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Smart Card Alliance Members: Members can access all Smart Card Alliance reports at no charge. Please consult the member login section of the Smart Card Alliance web site for information on member reproduction and distribution rights.

Government Agencies: Government employees may request free copies of this report by contacting info@smartcardalliance.org or by joining the Smart Card Alliance as a Government Member.

Table of Contents

About the Smart Card Alliance ____ *2*

Table of Contents ____ *3*

Executive Summary ____ *4*

Introduction ____ *6*

Existing Contactless Payment Applications ____ *7*

Hong Kong Octopus Card ____ 7

ExxonMobil Speedpass ____ 9

Visa Contactless Payment in South Korea ____ 11

MasterCard PayPass™ ____ 12

Contactless Payment Benefits and Costs ____ *14*

Contactless Payment Technology Options ____ *18*

Primary Contactless Payment Technologies ____ 18

ISO/IEC 14443-Compliant High-Frequency 13.56 MHz Contactless Smart Cards 18

ISO/IEC 15693-Compliant High-Frequency 13.56 MHz Contactless Smart Cards 20

Proprietary High-Frequency 13.56 MHz Technology 21

Proprietary Low-Frequency 125 to 134 KHz RF Technology 22

Proprietary Ultra-High-Frequency RF Technology 23

Alternative Contactless Technologies ____ 24

Infrared Solutions 24

Microwave Technology – Bluetooth 25

Carrier-Based Mobile 26

Near Field Communication 27

Key Technology Considerations ____ 28

Contactless Payment Transaction Models ____ *34*

Speedpass ____ 34

E-ZPass ____ 35

Contactless Payment Using Track 1 and Track 2 Magnetic Stripe Credit Card Data ____ 36

Contactless Credit/Debit Card Using EMV ____ 38

Stored Value Card ____ 39

Why Contactless Smart Cards? ____ *40*

Conclusion ____ *44*

References and Resources ____ *45*

Publication Acknowledgements ____ *47*

Appendix A: Contactless Transit Implementations ____ *48*

Smart Card Alliance © 2003

Executive Summary

Contactless Payment Represents a Growing Market

The latest trend in retail payment applications is contactless payment. Contactless payment systems are used successfully in Asia, Europe and North America and offer a number of advantages to issuers, retailers, and consumers. Contactless payment allows issuers to penetrate the cash payment market, enjoy increased customer transaction volume, and improve customer retention and loyalty. Retailers realize benefits due to faster transaction times, increased revenue, improved operational efficiency, and lower operating costs. Consumers enjoy the convenience of hands-free payment, the ability to pay for multiple services using one device, and the security of not having to display a card for payment.

Contactless payment applications are particularly attractive to retail segments where speed and convenience of payment are essential (for example, quick service restaurants, gas stations, convenience stores, parking facilities, transit services, entertainment venues and unstaffed vending locations).

Multiple Technologies Support Contactless Payment

Multiple technologies may be used to implement a contactless payment system. Candidate technologies include radio frequency, infrared, carrier-based mobile and Bluetooth technologies. Three types of radio frequency technologies are currently used, including: high-frequency 13.56 MHz contactless smart cards, low-frequency (100 to 300 KHz) devices and ultra-high-frequency (900+ MHz) transponders.

The choice of an appropriate technology is driven by issues such as what types of payment mechanisms the technology supports, whether the technology is commercially available and governed by international standards, what regulatory issues apply, how much investment is required, and how well the technology protects customer data and guards against erroneous transactions.

Various Transaction Models Support Contactless Payment

A contactless payment system can follow a variety of transaction models. Candidates include account-based payment, traditional credit or debit card payment, and stored-value payment. Each transaction model requires a different infrastructure investment and different participation by the consumer, retailer, acquiring processor, and issuing bank. Which transaction model is appropriate depends on the approach chosen to implement the system.

Contactless Smart Cards Offer an Excellent Choice for Retailers

Smart cards are being used for payment throughout the world, with Visa, MasterCard and JCB leading initiatives to extend the use of smart cards for contactless payment. The combination of standards-based technology, enhanced security features, availability of products and services from multiple vendors, potential to use the existing payments infrastructure, and

support from major financial industry players offer compelling benefits for payment implementations based on contactless smart cards.

About This Report

This report was developed by the Smart Card Alliance to describe contactless payment applications, technology options and transaction model alternatives. This report provides answers to commonly asked questions about contactless payment systems, such as

- What retail sectors can benefit most from contactless payment?
- What are example implementations of contactless payment and how successful have they been?
- What are the technologies that can support contactless payment?
- What are the business drivers for adopting contactless payment?
- Are there advantages to using contactless smart cards in contactless payment systems?

Introduction

The financial, retail, and transportation industries are all abuzz over the latest payment trend — contactless payment devices. These devices come in a variety of shapes and sizes, ranging from traditional plastic cards to key fobs, watches, and cellular phones. Major cities around the world already use contactless smart cards for transit payment, with many major cities in the United States also implementing or planning to implement contactless smart card-based automatic fare collection (AFC) systems.[1] In 2002, MasterCard, VISA and JCB also announced the availability of contactless payment options for traditional cash-only environments where speed is essential, such as quick serve and casual restaurants, gas stations, convenience stores, and movie theaters.

Because contactless payment is a new market using and promoting a range of technologies and transaction models, the terminology describing it can be confusing. This report defines "contactless payment" as the ability to perform a non-cash payment transaction without a physical connection between the consumer payment device and the physical point of sale (POS) terminal. Contactless payment may be implemented using different contactless technologies, including radio frequency (RF), infrared (IR), Bluetooth, and carrier-based mobile technologies. Three types of RF technologies are described in this report, including high-frequency 13.56 MHz contactless smart cards, low-frequency (100 to 300 KHz) devices and ultra-high-frequency (900+ MHz) transponders.[2]

This report provides information on current contactless payment applications and on the benefits and value proposition for retailers and issuers considering such a payment scheme. It examines the various available contactless technologies, transaction models and implementation approaches. Finally, it describes the advantages of contact and contactless smart cards as compared to other current payment mechanisms.

[1] See Appendix A for a summary of North American transit agencies implementing or planning to implement smart card-based systems.

[2] RF bands are defined as: low-frequency - 30 KHz to 300 KHz; high-frequency – 3 MHz to 30 MHz; ultra-high-frequency – 300 MHz to 3 GHz.

Smart Card Alliance © 2003

Existing Contactless Payment Applications

Contactless payment applications have existed for more than a decade. Since the 1980s, millions of toll-road users have used "long distance" contactless technology for prepaid accounts or customer billing. ExxonMobil's Speedpass™ was introduced in the mid-1990s, and over 6 million customers now use a key fob, vehicle tag or watch to pay for gas and convenience store items at more than 7,500 Exxon and Mobil stations in the United States, Canada, and Singapore.

A number of mass transit agencies are also in the process of moving from magnetic stripe cards to contactless smart cards for fare payment or are testing smart card-based systems. According to Datamonitor, the market for transit-related contactless smart cards will grow from $55 million in 2002 to $200 million by 2006.[3] Contactless smart cards are currently being used in many cities worldwide (including Hong Kong, Tokyo, Seoul, Pusan, Washington, DC, and Shanghai), with the majority of new transit fare payment systems planning to use contactless smart cards as the primary ticket media. In many of these cities, these contactless smart cards are expanding beyond transit-only payments to include contactless payment with local retailers.

This section describes several current contactless payment applications that are being used at the retail point of sale.

Hong Kong Octopus Card

The Hong Kong Octopus card, launched in 1997 as an electronic purse for public transportation, is the most successful and mature implementation of contactless smart cards used for mass transit payment. The card's acceptance and popularity have since extended its use to nearby retailers. Its success highlights two critical components of any payment strategy: strong self-service habits and the ability to leverage these habits to launch payment technologies for the general retail environment.[4] The Octopus card is a good example of a contactless transit payment application that is evolving into a general retail payment mechanism.

Octopus cards were developed as an automatic fare collection (AFC) scheme for Hong Kong's transit system. Over 9 million Octopus cards and 150,000 smart watches have been issued, and over 7 million transactions are recorded on a daily basis, for a daily transaction value of over HK$50 million (about US$6.5 million).[5] This contactless smart card ticketing system currently includes over 100 service providers, including all of the major transport operators (bus, taxi, subway, train, tram, and ferry services). Because Hong Kong's main transport operators are all partners in the Octopus card, kiosks are widely available, making it easy for customers to check the balance on a card and recharge it with cash or electronic payments. The use of the card has shortened queues at ticket barriers,

[3] "Access Will Overtake Transit as Contactless Card Application," *Card Technology*, October 2002, p. 25.
[4] Contactless Smart Card Schemes in the Asia Pacific Region," Asia Pacific Smart Card Association report, August 2002.
[5] Donald Davis, "The Contactless Wave," *Card Technology*, January 2003.

because the card doesn't have to be taken out of a bag or wallet — customers can just wave it past a scanner at a distance of several centimeters.

The first non-transit applications for the Octopus card allowed the card to be used for payment at photo booths located in the Mass Transit Railway (MTR) stations and pay phones operated by New World Telephone. After only 5 years, 25 percent of Octopus card transactions are unrelated to transit.[6] The card lets consumers make payments quickly and conveniently and is accepted by more than 160 merchants:[7]

- Park 'N Shop (Hong Kong's leading supermarket), Watson's, 7-Eleven, and Starbucks accept the Octopus card. Many fast food outlets already accept the card, and McDonald's is expected to accept it in the near future. Octopus charges a 1% commission on retail purchases.
- More than 3,000 soft drink vending machines in offices, schools, and shopping malls now have Octopus scanners. Sales have increased, as consumers make more impulse buys when they don't need to use cash.
- Pay phones, photo booths, and many car parks accept the card, avoiding the need for consumers to carry change. The card can also be used for admission to public swimming pools and other recreational centers.
- Nokia has launched a cover for one of their mobile phones that includes an embedded Octopus chip and antenna, enabling commuters to use their phone to make Octopus payments.

While Octopus cards are anonymous by default, over 500,000 personalized cards have been issued and are used for the Octopus Automatic Add-Value Service. Twelve Hong Kong banks and one credit card company support the automatic add-value service. Because each personalized card has a unique identification number, up to 40,000 cards are also being used as security passes at housing estates, for staff identification cards, and as loyalty cards.

The contactless Octopus card is based on Sony's FeliCa™ technology, a proprietary 13.56 MHz technology similar to but not compliant with the ISO/IEC 14443 standard technology. This technology has widespread acceptance in the Asia Pacific region, with over 25 million cards issued worldwide.[8] Terminals read the cards instantly, processing transactions in less than one-third of a second. On the MTR, a scanner at the ticket barrier loads data on the card that is then used by scanners at the exit gates to deduct the correct fare and show the remaining credit.

In 2002, the Asia Pacific Smart Card Association reported that 95% of the "economically active population" was using the Octopus card.[9] Travelers have found that the card provides increased convenience, allowing them to pass through fare collection points 15 to 20% faster, according to Octopus card statistics. The scheme has succeeded because it offers real convenience to cardholders.

The Kansai Thru Pass, a similar transit application using the FeliCa technology, is being rolled out over the next 5 years in the Japanese cities of

[6] Asia Pacific Smart Card Association, op. cit.
[7] Ibid.
[8] JCB Contactless Presentation, January 2003.
[9] Asia Pacific Smart Card Association, op. cit.

Kyoto, Osaka, and Kobe. JCB will issue more than 5 million Thru Pass cards to be used in a merchant base that includes 10,000 POS terminals.[10]

In the United States, the Washington Metropolitan Area Transit Authority (WMATA) has 325,000 SmarTrip contactless smart cards in circulation, used for payment throughout the Metrorail system and at all WMATA-operated parking facilities. WMATA has also entered into pilots that expand the use of the card to other applications. In a pilot agreement with First Union National Bank, 1,000 co-branded cards were issued in 2000 that could be used in WMATA's transit system (as a contactless smart card) and used as a debit card (with a magnetic stripe) for banking transactions or re-loading the card for transit use. The cards were re-issued to participants in 2002. Based on survey data gathered from the cardholders, consolidation of functions on a multi-application card was an attractive feature and would lead to increased use of the card. WMATA also entered into a pilot with the U.S. General Services Administration and U.S. Department of Education for a co-branded, multi-function transit-building access card. These pilots were initiated in 2000 and 2002, respectively, include approximately 2,000 cardholders between the two agencies, and continue to operate today.[11]

ExxonMobil Speedpass

Speedpass, introduced by ExxonMobil in 1997, was the first automated payment system to adopt radio frequency-based technology to help consumers make retail purchases. Today, over 6 million Speedpass customers frequent 7,500 Exxon- and Mobil-branded locations around the world. Over 92% of the Speedpass users report a high level of satisfaction.[12]

The ExxonMobil Speedpass project resulted from a 1993 Mobil study that concluded that convenience, friendly service, and recognition of loyal customers create consumer loyalty and additional spending. The benefits to the consumer are straightforward: no foraging for change or bills, no handling of credit cards, no paper receipt to sign or keep track of, and no personal identification number (PIN) to enter or remember. In general, the entire transaction is handled more quickly and the customer is in control at all times.[13]

Motorists enrolled in Speedpass use a key fob, watch, or transponder affixed to their vehicle's rear window to communicate securely with a gas pump or POS terminal. A reader integrated into the pump or terminal sends a signal to the customer's device, which replies with a unique identification code that is linked to a customer account. The customer is then authorized for payment, and the pump is activated, or a purchase can be made at the convenience store. Consumers do not pay for the Speedpass device, and there is no consumer service charge for using this technology to make payments.

Speedpass is recruiting key retailers in other sectors, such as grocery stores and fast-food restaurants, to use the payment technology. Selected Stop &

[10] *ContactlessNews*, Volume 1, Number 2, January 2003.
[11] Source: WMATA
[12] *Texas Instruments RFID eNews*, Issue No. 14, November/December 2002.
[13] Amy Cortese, "Toolbooth Technology Meets the Checkout Lane," *New York Times*, July 7, 2002.

Smart Card Alliance © 2003

Shop supermarkets began using Speedpass in 2002 for payment, coupons, and a loyalty program. During the past 2 years, over 430 McDonald's locations in the Chicago area have begun accepting Speedpass.

In December 2002, ExxonMobil Speedpass and Timex® released 4,000 timepieces featuring a miniature Speedpass transponder. The watch looks and functions like a regular watch, but enables customers to pay instantly and even more conveniently at Exxon and Mobil service stations.[14]

The RFID transponders used in the Speedpass devices (key fobs, watches, and window transponders) were designed by Texas Instruments and feature a digital signature encryption protocol with challenge/response authentication to ensure consumer protection. This technique makes it extremely difficult, if not impossible, to duplicate the transponder (tag) or the secret encryption key. According to Texas Instruments, even if the key were duplicated, it would only be valid for a single tank of gas.[15] The Speedpass system was also designed to ensure customer privacy and security. The customer's credit or check card number is not used by the Speedpass device or merchant POS terminal, maintaining the confidentiality of that information.

Customers at Exxon- and Mobil-branded service stations increased their purchases of gasoline by 15% after they became Speedpass users, resulting in a sales lift of 4%.[16] (Sales lift is measured as total gallons sold for the 12 months prior to implementing Speedpass compared with the 12 months after Speedpass was implemented at each location). This represents one additional gas purchase per month per customer.

Several other pilots are also in progress using payment systems similar to Speedpass. Shell Canada has launched its 'EasyPay' solution based on ISO/IEC 15693 technology from TI to over 400 service stations. McDonald's is conducting two pilots using RF-based contactless payment systems from other service providers. One involves using RFID technology by FreedomPay® at 32 outlets in Boise, Idaho and the other allows E-ZPass℠ customers on Long Island to use their E-ZPass toll transponders to pay at the drive-through window.[17] Similar trials are being conducted by Taco Bell® and KFC® using a product from a company called 2Scoot®. According to Ed Kountz, a senior analyst for emerging technology with TowerGroup, "Trials in so-called quick-service restaurants (aka fast-food joints) have resulted in a 15 to 30 percent 'bag lift'—the industry jargon for an increase in average order cost."[18]

Bank of America recently announced the QuickWave contactless payment pilot.[19] Launched in 2002 in Charlotte, North Carolina, the pilot includes 10,000 Bank of America employees and 15 downtown restaurants and shops. Participants pay for their purchases and accumulate loyalty points by using the card. The scheme is similar to Speedpass in that the contactless card references the user's bank account. QuickWave uses technology from FreedomPay and Inside Technologies that supports both the ISO/IEC 15693

[14] See Speedpass web site, http://www.speedpass.com.
[15] "Mobil Speedpass Goes Global as Mobil Singapore Rolls Out Asia's First RFID-Based Pay-At-The-Pump System," Texas Instruments press release, April 5, 1999.
[16] Matthew Miller, op. cit.
[17] Ibid.
[18] Matthew Miller, "Received Wisdom," *CommVerge*, November 1, 2002.
[19] *ContactlessNews*, Volume 1, Number 2, January 2003.

and ISO/IEC 14443 Type B contactless smart card standards.[20] The pilot will continue through March 2003.

Visa Contactless Payment in South Korea

Since 1998, approximately 6 to 7 million Visa-branded contactless cards have been issued by several large Visa members in South Korea. These cards contain a chip, which is used for contactless payment in the Seoul transit system, and a magnetic stripe, which is used for regular credit card payments. The popularity of transit applications on credit cards means that contactless chips have become a standard feature for the majority of new credit cards issued to residents of Seoul. Several other major cities in South Korea (Busan, Jeonju, Inchon, and Ulsan) have also deployed Visa credit cards coupled with a contactless transit application. However, unlike the cards used in Seoul, these cards are issued as "dual-interface" cards in which a contact-based electronic purse (on a chip) is offered along with a contactless transit application (also on a chip).

In 2002 Visa introduced the dual-interface GlobalPlatform (GP) card, based on Philips technology. Unlike previous dual-interface cards, the new GP cards allow applications to be downloaded, modified, and deleted after the card has been issued. The cards also support VSDC and Visa multi-functionality. Three major districts in South Korea, (City of Daejon, City of Gwangju, and Chungnam Province) have adopted these dual-interface GP cards. Issuance begins in 2003, with a target of up to 2 million cards. In addition to the ISO/IEC 14443 and MIFARE-based transit application, the card will also carry VSDC (EMV credit and debit), digital ID, Visa Cash e-purse, and loyalty applications. Other cities that have been issuing proprietary transit cards are planning to migrate to Visa's dual-interface Global Platform cards.

Visa continues to work very closely with S-1/Samsung Electronics in several areas to provide VSDC payment and multi-function capabilities through the dual-interface smart card chip. Current programs include contactless access control to corporate buildings for Samsung employees and their families and contactless access for residents of apartment buildings in several major South Korean cities.

SK Telecom, the largest mobile telecommunications service provider in South Korea, launched the second phase of their Moneta card program in December 2002. The Moneta card now supports Visa payment at the point of sale using an IR beam or signal sent from mobile telephone handsets to upgraded merchant terminals. Plans are in place to expand this program and include contactless Visa payment in 2003. By the end of 2003, it is anticipated that approximately 400,000 terminals will be upgraded to support IR and contactless smart card technology and approximately 2 to 3 million handsets will be deployed.

Two other South Korean telecommunications providers, KTF and LGT, have indicated that they will also provide Visa payment at the retail POS using infrared and contactless smart card technology in 2003.

[20] *BiometricTech News*, January 16, 2003.

MasterCard PayPass™

MasterCard's PayPass, announced in December 2002, eliminates the need for users to swipe their cards through a reader. Consumers tap their payment cards on a specially equipped merchant terminal (or wave them at the terminal) that then transmits the payment details wirelessly. The new solution is targeted for traditional cash-only environments where speed is essential, such as quick service restaurants, gas stations, convenience stores, and movie theaters.

Chase, Citibank, and MBNA are working with MasterCard in a MasterCard PayPass trial in Orlando, Florida. Consumers can use the PayPass card at a variety of participating Orlando merchants, including Boater's World, Chevron, City of Orlando Parking, Eckerd, Friendly's, Loews Universal Cineplex, McDonald's, Ritz Camera, and Wolf Camera. Additional retailers are expected to begin participating in early 2003. The MasterCard PayPass card also includes a magnetic stripe, allowing consumers to use it at any location that accepts MasterCard.

Recent MasterCard consumer research reveals the following reactions to PayPass:[21]

- 63% of the consumers surveyed said that they would "definitely" or "probably" use MasterCard PayPass if their bank offered it to them.
- Consumers who said that they would definitely use the card indicated that it will replace cash in more than half (53%) of their transactions.
- PayPass is perceived to be "innovative" and "fun to use," as well as an enhancement that "would make shopping less of a hassle."

The MasterCard PayPass card uses ISO/IEC 14443 standard technology (Types A and B) to securely transmit Track 1 and Track 2 payment information from the card to the merchant terminal using RF. This eliminates the need for a cardholder to present the card to the merchant to swipe through a reader, allowing the cardholder to remain in control of the card. The payment transaction is then processed through the existing MasterCard acceptance network. The simplified approach of using Track 1 and Track 2 data allows merchants to cost-effectively retrofit their current magnetic stripe POS terminal to start accepting PayPass cards.[22] This is accomplished using an RF adapter that involves no POS software change. MasterCard plans to introduce MasterCard PayPass to additional markets when the Orlando trial is completed.

Summary

Figure 1 summarizes the technology and device formats used by each of the applications discussed in this section.

[21] "New MasterCard PayPass Utilizes Contactless Payment Technology," MasterCard press release, December 12, 2002.
[22] "U.S. Smart Card Breakthrough," The Nilson Report, January 2003.

Figure 1: Featured Applications and Corresponding Technology

Featured Application	# of Cards Issued	Technology	Form Factor
Hong Kong Octopus Card	9+ million	Non-standard 13.56 MHz (FeliCa)	Plastic card
ExxonMobil Speedpass	6+ million	Low-frequency RF (TI)	Key fob, wrist watch, window transponder
Visa Contactless Payment	7+ million	ISO/IEC 14443 13.56 MHz, Infrared	Plastic card, mobile phone
MasterCard PayPass	Pilot phase	ISO/IEC 14443 13.56 MHz	Plastic card

Contactless Payment Benefits and Costs

In the United States, contactless payment is an emerging market. A number of contactless technologies are being implemented, various payment processes are supported, and both pilot and commercial services are available. While the market is new, there is already evidence that retailers can see significant benefits from implementing contactless payment and that consumers value its increased convenience and speed.

This section describes the general business benefits and costs of implementing contactless payment for retailers and issuers. It does not attempt to quantify the business case, since actual benefits and costs vary by retail segment and by the technology used.

Retailer Benefits

Retail segments in which speed and convenience of payment are essential can realize significant benefits from contactless payment. These segments include: quick service restaurants, especially those with drive-through service; gas stations; convenience stores; parking facilities; transit services; entertainment venues; amusement parks; and unstaffed vending locations (for example, vending machines or ticket kiosks).

While the business drivers differ for each retail segment, early contactless payment implementations have demonstrated the following benefits:

- Faster transaction times
- Increased revenue
- Improved operational efficiency and lower operating costs
- Better customer information
- Payment device branding or co-branding
- Competitive differentiation

Faster transaction times are achieved by moving customers more quickly through the transaction process. Contactless payment is faster than both cash and traditional magnetic stripe credit card transactions. By eliminating the need for consumers to extract cash or cards and for retailers to make change or swipe a card, TowerGroup estimates that contactless payment using RFID fobs can save 10 to 15 seconds per transaction.[23] Sue Gordon-Lathrop, vice president for emerging consumer environments at Visa International, has stated that contactless payment can decrease drive-through transaction time by 90 seconds..[24] In some retail segments, faster customer service may translate directly into increased revenue.

Increased revenue results from increased spending per transaction, increased frequency of purchase, and increased loyalty (when the merchant becomes the customer's preferred retailer). Customers also potentially have access to more funds when they pay using a contactless payment device instead of cash. ExxonMobil has stated that a 4% increase in sales resulted from using Speedpass.[25] Other vendors and retailers implementing

[23] Edward Kountz, "RFID Payment Fobs at Point of Sale: The Early Face of M-Payments in North America," Tower Group,, March 2002.
[24] "Visa, MasterCard diverge on proximity payments," *European Card Review*, August 2002.
[25] Matthew Miller, op. cit.

contactless payment have reported 15 to 30% increases in sales after implementing contactless payment.[26 27 28 29]

Improved operational efficiency and lower operating costs result from reducing overhead and resource requirements at merchant locations, reducing cash handling and pilferage costs, and improving reliability of payment terminals.

Better customer information enables the retailer to better understand customer behavior by collecting data that could not be collected with cash purchases.

Payment device branding or co-branding means major retailers can benefit from relationships with issuers, adding the retailer brand to the payment device and achieving increased visibility with consumers.

Competitive differentiation attracts new customers by providing more convenient payment methods.

Retailer Costs

As with any new payment method, retailers will need to invest in new infrastructure and processes to implement contactless payment. Costs to be considered include both installation and ongoing costs:

- **Cost to upgrade POS hardware and software** to accept contactless payment. This cost depends on the technology chosen (currently ranging from tens to hundreds of dollars) and will change over time as terminal vendors integrate contactless payment capability directly into new terminals.
- **Cost to upgrade retailer host systems** to support new transaction data and to route transactions to the appropriate payment processors. Whether there is a requirement to upgrade depends on which contactless payment transaction model is used. Some contactless payment solutions use existing credit and debit networks and standards, while others require new payment processors or gateways.
- **Cost to train customer service staff**. Customer service staff will need to be trained to use the contactless payment terminal and process and to help customers use the contactless devices.
- **Marketing and promotion costs**, to encourage customers to use new contactless payment options.
- **Transaction fees** for processing contactless payments. Fees will depend on the transaction model and service providers offering contactless payment processing
- **Maintenance and management costs** associated with the new payment solution.

[26] Amy Cortese, op. cit.
[27] Jon Karlen, "Contactless Micropayments," *Wireless Future Magazine*, September/October 2002.
[28] "Gilbarco Wants to Help Gas Stations Pump Up Profits," *RFID Journal*, June 2002.
[29] John Elliott, "Losing contact: the transactions of the future are disappearing into thin air," *Cards Worldwide*, March 15, 2002.

Issuer Benefits

There are a number of different potential issuers for contactless payment devices, including: transit agencies (e.g., Washington, DC, Hong Kong); transit outsourcing providers (e.g., Transys London); new companies focused on providing contactless payment devices and services (e.g., Speedpass); traditional credit/debit card issuers (e.g., MasterCard and Visa members); and retailers who may offer their own branded payment card or device. Each of these issuers will have different drivers for issuing contactless payment devices. Key drivers are the following:

- **Penetration of the cash payment market**. In the United States in 2001, cash was used for approximately 20% of total consumer payments.[30] Issuers can add transaction volume to existing payment cards or reduce cash handling requirements by replacing cash payments with a contactless payment method that is connected with another form of electronic payment mechanism (i.e., credit or debit card or bank account).
- **Increased customer transaction volume**. By making it more convenient for customers to pay, issuers can realize increased transaction volume as consumers use the contactless payment device more often. WMATA has also found that the contactless AFC payment card reduces the consumer's perceived cost of a transit trip.
- **Improved customer retention and loyalty**. The consumer reaction to initial implementations of contactless payment has been very favorable. By offering a payment device that increases the convenience and speed of the transaction process, issuers may experience better customer retention and loyalty, becoming the payment device issuer of choice.
- **Co-branding opportunities.** Issuers entering the contactless payment market have the opportunity to strengthen relationships with major retailers by offering co-branded payment devices.
- **New service opportunities.** Contactless payment issuers can provide new services to retailers that include payment processing and other value-added capabilities, generating new or incremental revenue streams.

Issuer Costs

Issuers must also consider the cost of implementing new contactless payment devices and services. Issuer costs include the following:

- **Cost of the contactless payment device.**
- **Personalization and life cycle management costs** for the payment device.
- **Operations costs** to accommodate the expected risk profile of contactless payment transactions.
- **Transaction processing infrastructure costs** if changes or investments are required to process new contactless payment transactions.
- **Cost of training customer service staff** to answer consumer questions and address any issues created by using the new contactless payment devices.

[30] "Consumer Payment Systems," *The Nilson Report*, Issue #777, December 2002.

Summary

While the benefits of contactless payment to the issuer and retailer are clear, the business case needs to evaluate the actual benefits and costs of a specific contactless payment technology, transaction model, and service. The business case must also compare the results to the cost of the payment methods already in use. For example, the cost/benefit comparison for a retailer who is converting customers from cash to contactless payment will be different than the comparison for a retailer who is converting customers from credit or debit cards (using magnetic stripe or contact smart cards). Contactless payment implementations may also benefit from linking with large-scale transit payment programs that are already underway and that could underwrite card issuance and point of sale terminal deployment (though the harmonization of application requirements and impact on business cases need to be thoroughly considered). As both retailers and issuers gain more experience with early contactless payment implementations, the business case will be proven for different technologies and transaction models.

Contactless Payment Technology Options

Contactless payment requires a wireless information exchange between the consumer's payment token and a payment terminal or infrastructure device. Contactless payment can be enabled using a variety of technologies and payment tokens in many different forms. Each technology has tradeoffs that affect the feasibility and effectiveness of using it in the North American retail environment.

The available technologies support both radio and optical information exchange. Current RF-based alternatives include contactless smart cards, RFID tokens, RF transponders, Bluetooth-enabled devices, and carrier-based mobile solutions (such as mobile phones). Optical alternatives include IR-enabled devices such as PDAs and mobile phones that execute payment transactions over an IR link between the device and POS terminal.

The following two sections summarize the primary current contactless technologies and alternative solutions.[31]

Primary Contactless Payment Technologies

The three primary contactless payment technologies include: high-frequency 13.56 MHz solutions; low-frequency proprietary solutions like Speedpass; and ultra-high-frequency RF solutions like those used for toll applications.

ISO/IEC 14443-Compliant High-Frequency 13.56 MHz Contactless Smart Cards

ISO/IEC 14443 is a contactless technology standard for "proximity" smart cards operating at 13.56 MHz. This standard specifies the characteristics of cards with an operational range of up to 4 inches (10 centimeters). The technology was originally designed for electronic ticketing and electronic cash applications. For these applications, short operational ranges and fast transaction speeds are critical. These same market requirements led ISO/IEC 14443 to be adopted for transit, off-line purchase, vending, and physical access control applications.

Advantages and Disadvantages

ISO/IEC 14443 was initiated in 1994 to standardize contactless proximity cards and finalized in 2001. To date, approximately 250 to 300 million contactless smart cards have been shipped based on the ISO/IEC 14443 standard.[32] The majority of these cards are used in transportation applications for automatic fare collection, with the largest installations in Asia. ISO/IEC 14443 cards are supplied by the largest base of semiconductor suppliers and card manufacturers.

---

[31] Note: The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this section concerning contactless technologies and the status of their deployment is accurate as of the date of this paper.

[32] "Contactless Smart Card Technology for Physical Access Control," Avisian, Inc., April 1, 2002 and Philips Semiconductors.

A number of different ISO/IEC 14443-compliant card products are available, offering a range of characteristics at a number of price points. These characteristics include compliance to different levels of the standards, differing encryption and authentication schemes, and differences in processing power and card resources. Readers are available that can interoperate with the range of available card products, allowing an issuer to provide a choice of solutions and a migration path to more powerful devices if required.

ISO/IEC 14443 does not specify a standard for contactless link encryption or card-to-reader authentication. However, virtually every semiconductor vendor provides options to provide these security services. A common encryption/authentication protocol used with ISO/IEC 14443 Type A is the MIFARE protocol. An independent certification institute offers MIFARE compliance testing, ensuring that certified products from multiple vendors will work together.[33]

The 10 centimeter operational range of ISO/IEC 14443 may be an advantage since the act of payment is more intentional and close proximity of the card to the reader helps limit unintended communication.

The 106 Kbps data rate of ISO/IEC 14443 cards is also considered an advantage in that more bandwidth is available for stronger security, larger amount of application data and reduced time in field.

Contactless microcontroller (MCU) cards that comply with ISO/IEC 14443 offer an excellent combination of interoperability and security. New dual-interface or contactless MCU cards fully comply with ISO/IEC 14443 (through part 4 of the standard). As a result, contactless and dual-interface smart cards have the same level of interoperability as contact smart cards. For example, dual-interface cards made available by Visa can execute the same financial applications in either ISO/IEC 7816 contact or ISO/IEC 14443 contactless mode. ISO/IEC 14443 MCU-based smart cards offer security features equivalent to those offered by contact smart cards. Features such as memory firewalls that separate applications on the card, encryption, sensors, tamper-resistance, and crypto coprocessors provide robust security for transactions.

Contactless wired logic technologies are also available in the market and can comply through Part 3 of the ISO/IEC 14443 specification. While these products cannot support the ISO/IEC 7816-like Part 4 protocol layer, they do offer a lower price point and faster performance. Depending upon the needs of the issuer and the products or applications to be supported, these could be a cost-effective choice.

ISO/IEC 14443-compliant readers are available from multiple vendors. In addition, several readers are capable of reading both ISO/IEC 14443- and ISO/IEC 15693-compliant cards, with a few supporting an even broader range of technologies.

The financial industry is supporting contactless payment solutions based on ISO/IEC 14443. Visa International has endorsed a global payment specification for contactless cards based on ISO/IEC 14443, and a number of

[33] Ibid.

trials in Asia are already underway or planned.[34] MasterCard International has also implemented contactless technology based on ISO/IEC 14443 for use by its members and in the PayPass pilot in Orlando, Florida.[35]

Summary

The adoption of ISO/IEC 14443-based contactless solutions by payment associations, the security features of the technology, and its widespread use in payment applications make ISO/IEC 14443-compliant contactless smart cards well suited for any open or closed payment application.

ISO/IEC 15693-Compliant High-Frequency 13.56 MHz Contactless Smart Cards

ISO/IEC 15693 is a contactless technology standard for "vicinity" smart cards operating at 13.56 MHz. This standard specifies the characteristics of cards with an operational range of up to 1 meter, although practically speaking the range is limited to 70 centimeters or less. Traditionally, ISO/IEC 15693-compliant tokens have been used for tagging, ticketing, and access control applications. As these tokens become more capable and are deployed more widely, however, new applications are being considered, especially for closed-system enterprise payment (for example, as part of multi-application employee badging systems and for some retail solutions).

Advantages and Disadvantages

ISO/IEC 15693 was initiated in 1996 to standardize contactless vicinity cards and finalized in 2001. The most common application identified for these cards, to date, is multi-application enterprise access control cards. ISO/IEC 15693 cards are supplied by a growing number of semiconductor suppliers and card manufacturers.

Since ISO/IEC 15693, like ISO/IEC 14443, does not define any security protocols or requirements, vendors have implemented a number of security features, including encryption of stored data, authenticated access to card memory and card-to-reader mutual authentication.

The longer range afforded by ISO/IEC 15693-compliant systems is viewed as very beneficial by drive-through restaurants and retail, two of the fastest growing contactless payment sectors. The longer range is also considered beneficial by enterprises that support parking or vending applications. On the other hand, any technology with a longer range may be perceived to have a potential security risk for two reasons: the lack of payment "intentionality" on the part of the token holder, and the potential that someone with a compatible reader could stand a few feet away and access data on the card (though this risk exists in differing degrees with all contactless technologies). Appropriate selection of security services or adjustment of operational ranges can mitigate this risk.

The ISO/IEC 15693 standard supports a maximum data transfer rate of 26 Kbps (a function of operational range). Due to the longer operational range, the card may be in the RF field for a longer period of time, allowing enough

[34] John Frank, "Visa selects ISO 14443 as its standard for global contactless payments," *ContactlessNews*, December 2002.
[35] MasterCard, op. cit.

time for communication between the reader and card even with this lower data rate. Requirements for transaction time, amount of data in each transaction and security services must be considered to determine whether this data rate is sufficient to meet payment application requirements.

ISO/IEC 15693- compliant readers are available from multiple vendors. In addition, several readers are capable of reading both ISO/IEC 14443- and ISO/IEC 15693-compliant cards, with a few supporting an even broader range of technologies.

Summary

ISO/IEC 15693-compliant contactless smart cards are currently well suited for closed-system payment applications. This technology is especially attractive where a longer read range is beneficial or mandatory; shorter ranges are also achievable. The perceived security risks for payment and lack of endorsement by any payment association or major financial institution have resulted in this technology being used for payment primarily in closed systems today. As demand for payment requiring longer operational ranges increases, ISO/IEC 15693-based solutions may emerge.

Proprietary High-Frequency 13.56 MHz Technology

Non-standard 13.56 MHz cards and readers are currently available that are used extensively for transit applications in Asia Pacific markets (such as Hong Kong and Japan) and, to a more limited extent, in the United States. The most prominent examples of this technology are the FeliCa card, developed and promoted by Sony, and the GO CARD®, developed by Cubic Transportation Systems, Inc.

FeliCa Card

The FeliCa card is used by the Hong Kong Octopus card transit system, the New Delhi Metro, the Singapore Land Transit Authority, and by the majority of Japanese transit agencies. The FeliCa card uses the same frequency and form factor as ISO/IEC 14443-compliant cards but differs in some technical specifications. In Hong Kong, the FeliCa card is also increasingly being used for non-transit payment applications (for example, quick service retail and vending applications). Sony is promoting FeliCa with an electronic purse in Japan and other countries.

Several vendors are licensed to produce FeliCa-compliant cards and readers. The joint Philips and Sony Near Field Communication development could help drive the use of this technology beyond the Asia Pacific region.

Cubic GO CARD

The Cubic GO CARD is used by a number of large transit operators and has been used in several North American pilot transit projects. GO CARD technology uses the same frequency, modulation scheme, bit coding and form factor as ISO/IEC 14443 Type B-compliant cards but differs in other technical specifications. The technology's functional capabilities are tailored for high-speed, tear-proof transit applications and large storage requirements. Cards are available from a variety of card manufacturers

licensed by Cubic and Cubic's Tri-Reader® supports communication with ISO 14443 Type A and B cards and the GO CARD.

Advantages and Disadvantages

The primary advantage of proprietary 13.56 MHz technology is the installed card base and reader infrastructure that exist within specific geographic regions. Retailers in cities that are implementing contactless smart cards for transit payment could consider teaming with their local transit authority to offer contactless payment and take advantage of the broad issuance of cards to local consumers (though the harmonization of application requirements and impact on business cases need to be thoroughly considered).

The installation of readers that handle multiple card types provides issuers with additional flexibility, allowing multiple card types to be used with a common infrastructure.

The primary disadvantage is the lack of standards, which leads to interoperability issues among implementations. This may not be a disadvantage to a local transit agency, but should be taken into consideration by issuers and retailers when evaluating contactless technology.

Summary

Proprietary 13.56 MHz technologies tend to be suitable for use in specific geographic locations where interoperability with existing infrastructure is important. Proprietary technologies can also be used successfully in areas where global contactless payment is not a requirement (e.g., within countries or among cardholders where travel beyond a single city, region or country is infrequent).

However, the lack of standards compliance and transit operator-specific implementations suggests that adoption for use in more open systems or global payment environments may be limited.

Proprietary Low-Frequency 125 to 134 KHz RF Technology

Low-frequency RF technologies operate at less than 300 KHz. These generally use a unique ID within the application, so are most often referred to as RFID technology. Such technologies have been used extensively for security applications such as automobile immobilizers and for access control.

Speedpass is an example of the use of low-frequency RFID technology for payment in North America. The Speedpass technology operates at 134 KHz and can achieve ranges up to 10 cm, but with relatively low data transfer rates.

Advantages and Disadvantages

Low-frequency RFID technologies have no established communications standards at present and very limited processing power on the RF tag. They can also have potentially longer read ranges, though this is often addressed through the design of the antenna (to limit range). For these reasons, this technology may be perceived to have a potential security risk, unless

addressed for a given application.[35] The most predominant form factor used for low-frequency RFID payment is the key fob, but both automobile-mounted tags and tags embedded in watches are also available commercially. The auto tags are active tags, requiring a battery that must be replaced every 3 to 4 years.

There are no global standards for the technology; however ISO/IEC 18000-2 is currently in the process of being defined. Solutions are typically available only from limited sources.

Summary

The use of low-frequency RFID technology for contactless payments appears to be best suited for closed-system applications. A retailer selecting this technology could implement its own solution or partner with a contactless payment service provider (such as Speedpass or FreedomPay). Electing to join an existing network has the advantage of acquiring an installed base of users and an infrastructure and fulfillment system. Implementing a retailer-specific solution has advantages in terms of brand differentiation, promotion and overall control, and disadvantages in terms of interoperability and added costs of implementation and promotion. Given the lack of standards, lack of endorsement by payment associations, and perceived security risks, this technology does not appear to be appropriate for high-value payment or more general retail applications.

Proprietary Ultra-High-Frequency RF Technology

Systems based on ultra-high-frequency RF typically operate in the ISM band (902 to 928 MHz in the United States) and have an operational range of anywhere from 3 meters to more than 10 meters. These generally use a unique ID within the application, so are also referred to as RFID technology. The best example of the use of ultra-high-frequency RF technology that is applicable to payment applications is the use of RF transponders to pay highway tolls, such as the E-ZPass℠ system (used in the northeastern United States), TollTag™ (used in the Dallas metropolitan area), and FasTrak™ (used in California).

This technology could also be used for some forms of retail payment in conjunction with its use for paying highway tolls. For example, one McDonald's franchisee is participating in a trial using TollTag technology at five drive-through McDonald's restaurants in the Dallas area and a Long Island McDonald's is using E-ZPass. The consumer benefits from being able to access additional hands-free services without having to acquire an additional token. The toll operators will presumably increase revenue from the services provided to the retailers.

Automobile-mounted transponders can also be used in conjunction with smart cards (a payment card could be inserted into a transponder slot). This type of combined technology is used quite extensively in Singapore but is not currently deployed in North America.

[35] Note: Proprietary vendor-specific low-frequency RF security features are available.

Advantages and Disadvantages

Security for high-frequency RFID systems is limited or nonexistent. The transponders for these systems used in tolling applications are typically active devices, though passive transponders could be used for consumer payment applications requiring limited read range. The ultra-high-frequency and low power requirements translate into very small, efficient devices with high bandwidth between transponder and reader. Some devices may be capable of limited channel encryption or device authentication, but in general, security is an issue since most of these devices have not been developed for consumer payment applications. The long read ranges and limited security also contribute to the perception that a consumer could be charged inadvertently for fuel or services or maliciously defrauded.

The transponder devices can be very inexpensive, but the readers are typically more expensive than the readers required by other RF technology. The lack of a suitable ISM band at these frequencies also limits the use of this technology for global applications. Because there are no global standards for this technology, solutions are typically available from a single source only. Progress is being made on an open 5.9 GHz standard for tolling and other vehicle-oriented payment applications; this standard is targeted as an ISO/IEC sub-standard for global use.

Summary

The use of ultra-high-frequency RF tags for contactless payments appears best suited for closed-system payment applications like tolling and, potentially, for retail or payment operations linked to the toll system. The ability of the technology to operate at long ranges supports a positive user experience in executing drive-through transactions. However, given the lack of standards, lack of ISM band for global use, lack of endorsement by the financial industry, and potential security issues, this technology does not appear to be appropriate for high-value payment or more general retail applications. The required form factor and requirement to (typically) mount the tag semi-permanently also limit the general usefulness of this technology for payment.

Alternative Contactless Technologies

Alternative contactless technologies include IR solutions, Bluetooth, carrier-based solutions, and the joint development work by Philips and Sony called Near Field Communication.

Infrared Solutions

IR solutions offer an opportunity to use the more than 330 million IR-enabled mobile devices worldwide for payment purposes. Consumers are not only carrying these devices more frequently, they are also comfortable using IR, especially given the nearly omnipresent electronic remote control. IR-enabled devices can support operational ranges up to 2 meters, but devices that support ranges of 20 to 30 centimeters consume 10 times less power than the longer range devices. IR data transmission rates range from 9.6 Kbps with primary speed/cost steps of 115 Kbps up to a maximum speed of 4 Mbps.

Consumers are expected to be able to use their IR-enabled mobile phones and PDAs to make payment at the physical retailers. Many of the mobile phones being released today are programmable and could allow consumers to maintain a mobile wallet with various credit, debit, pre-paid, and loyalty cards securely stored in memory. Consumers would then choose a payment type using a simple menu at the time of payment

Trials of payment applications using IR are being carried out at a number of different locations, including South Korea and the University of Southern California (USC), with additional pilot projects planned for Japan. In South Korea, all three telecommunications providers (SKT, LG, and KTF) are participating in Visa contactless IR payment trials. In these implementations, Visa payment information resides in the handset of the telephone, and the consumer beams the Visa payment information to a POS terminal. The purpose of these pilot implementations is to test consumer and merchant acceptance of the new technology. In the planned USC pilot, a mobile phone-capable PDA can be linked to a USC Credit Union account to make payments at IR-enabled POS sites on campus. This is a hybrid payment approach involving carrier-based mobile and IR for the actual payment link.

Advantages and Disadvantages

The use of IR presents significant challenges. Different devices do not interoperate. In many devices, the IR port is currently disabled, requiring manual customer activation. There is also no easy way to download software to control the ports.

In addition, IR provides no link level security. Low-level transaction security is provided by the consumer's intention to conduct a payment transaction and the fact that it is difficult to intercept data being transmitted by a line-of-sight, narrow-angle beam. Application-layer security must be provided for stronger encryption or authentication service.

Summary

The Infrared Data Association® (IrDA®) is actively promoting interoperability of IR devices, and its Financial Messaging (IrFM) working group has developed Point and Pay Profiles[37] for payment applications. Visa is backing a variation of this profile, called the Visa Financial Messaging Profile for Proximity Payment.[38] When new IR-enabled mobile devices that support these standards are introduced, infrared-based contactless payment may become more widely deployed. However, the current interoperability issues and absence of widely adopted standards suggest that IR will not be practical for retail payment transactions in the near term.

Microwave Technology – Bluetooth

Bluetooth™ is a wireless RF technology designed as a small form factor, low-cost solution to connect mobile computers, mobile phones, and other portable handheld devices to the Internet. Bluetooth operates in the 2.45 GHz ISM band and has an operational range of 10 to 80 meters with a data

[37] See http://www.irda.org/news/fmupdate.asp
[38] See http://international.visa.com/fb/vendors/standspecs/downloads/proximity/main.jsp

transmission rate of up to 1 Mbps. After many years of development, there is finally strong growth in Bluetooth-enabled devices for different applications.

Advantages and Disadvantages

Bluetooth offers the advantage of longer-range transmission but has the disadvantage that the technology was developed for networking, not point-to-point localization. This means than any Bluetooth tag could be linked to multiple POS recipients. Localization processes can be implemented to address this issue, but at the expense of time and user experience.

Payment has not been a focus of the Bluetooth community to date. There were some earlier trials of payment applications based on Bluetooth in northern Europe, but there has not been any recent activity.

Summary

The lack of focus on payment, the lack of endorsement by the financial industry, and the lack of any available technical solutions suggest that using Bluetooth for retail payment transactions is not practical in the near term.

Carrier-Based Mobile

The use of carrier-based mobile devices (such as mobile phones) for payment applications seems a natural step, given the increasing use of the technology. Many telecommunication operators, suppliers, and infrastructure vendors have participated in a myriad of payment pilot projects. These pilots have tested wireless Internet payment, payment for vending and ticketing, and payment at brick and mortar establishments. The technologies used have involved a variety of approaches, including using a phone's IR port, using GSM SMS messages for payment authorization, using dual-slot phones for a payment smart card, and embedding RFID technology in the phone.

Current Status

None of the payment pilot projects has been particularly successful for a number of reasons, including lack of interoperability, difficulty of use, and high total cost of ownership. The situation in North America has an even greater potential for interoperability issues: numerous different technologies are in use by mobile operators (including GSM, PCS, TDMA, and CDMA), and the telecommunications environment is changing rapidly as newer broadband technology is deployed. The use of carrier-based mobile payment also raises a host of consumer experience and business issues, including how the consumer initiates the transaction, who "owns" the customer and how the costs of fielding solutions are covered. However, the major stakeholders continue to take an active interest in mobile payment, as is evidenced by the work of the Mobile Payment Forum.[39]

Summary

Given the lack of standards for mobile payment, the continuing technical and business challenges, and the lack of critical mass in any one particular

[39] See http://www.mobilepaymentforum.org.

payment approach, mobile payment can be eliminated as a practical alternative in the near term.

Near Field Communication

In September 2002, Philips and Sony announced joint development of a new near-field radio frequency communication technology called Near Field Communication (NFC).[40] The technology is designed to enable short-range communication networks between consumer devices with an NFC interface. The goal is to greatly improve wireless access to data and services. Ultimately, Philips and Sony intend to build an open infrastructure of NFC-compliant devices that incorporate smart key and smart card reader functions, providing a convenient method of implementing services such as payment (including credit card payment), ticketing, and accessing online entertainment content (such as gaming).

The wireless NFC technology will operate at 13.56 MHz across a distance of up to 20 centimeters. The technology will allow any kind of data to be transferred between NFC-enabled devices, such as mobile phones, digital cameras, PDAs, PCs, laptops, game consoles, or PC peripherals, at speeds fast enough to transfer high-quality images. With communication speeds of up to 212 Kbps, the NFC technology is expected be compliant with Philips' MIFARE and Sony's FeliCa contactless smart card technologies. Philips and Sony have stated that they will promote the NFC technology as an open standard in order to integrate it into consumer devices, including those built by other manufacturers in the electronics, PC, automotive, and other industries.

Once this technology is more completely specified and standards are proposed, it may be practical to consider it for retail payment applications. Understanding the potential of NFC may play a part in longer-term interoperability and application planning when implementing a contactless payment system in the near term.

[40] "Philips and Sony Announce Strategic Cooperation to Define Next Generation Near Field Radio-Frequency Communications," Philips press release, September 5, 2002.

Key Technology Considerations

Selecting a technology to implement a contactless payment system requires consideration of multiple key issues:

- Does the technology support the required payment mechanisms?
- What technical characteristics and features are important and how do they affect the customer experience?
- Is the technology commercially available today?
- What investment is required for implementation?
- What types of risks does the technology introduce or protect against and how do the risks affect the business model?

Supported Payment Mechanisms

In theory, contactless technology can support virtually any payment mechanism, including traditional credit and debit payments, pre-authorized account-based payment, and stored value payment.

Credit and debit transactions require the participation of one or more financial institutions and the participation or approval of a payment association. Contact smart card credit and debit payment based on the EMV standard is gaining rapid acceptance in Europe and Asia. In North America, the three major cards associations (American Express, MasterCard and Visa) have established contact smart card programs with significant issuer participation. The stronger security inherent in EMV could help drive increased offline sales (e.g., vending and kiosk-type payments). The Smart Card Alliance white paper "Smart Cards and the Retail Payments Infrastructure: Status, Drivers and Directions" has more information on key considerations for implementing EMV.

A pre-authorized system requires some level of certification and oversight by a participating financial institution or payment association. There are two types of pre-authorized accounts, each typically linked to a financial payment card or account. In one case, transactions are processed immediately by the financial institution. In the other case, pre-defined transaction limits are established and the account is replenished when its value reaches the lower limit.

Stored value systems are the predominant payment mechanism used by transit systems. Currently, all stored value systems are proprietary, although there is a major drive in Europe to promote the Common Electronic Purse Standard (CEPS). Stored value systems should not be discounted because they are proprietary. They have several favorable characteristics, including support for anonymous payment, fast transaction speeds with offline capability and, depending on the transaction processing model, the potential for limiting or avoiding transaction fees.

The key considerations for determining an appropriate payment mechanism include:

- Understanding maximum transaction value.
- The availability of proven technology for implementation.
- Knowing where fraud liability lies.
- Knowing what transaction fees will apply.

- Understanding what type of online processing and networking will be required.

It is also important to clearly understand what strategies are appropriate for risk mitigation and what type of financial oversight will be mandated.

Technical Characteristics

Selecting a contactless technology with the appropriate technical characteristics depends in part on what type of retail operation is to be supported. For example, transactions in traditional retail operations are typically more leisurely, and there is potentially more physical space available for a consumer to complete the transaction comfortably (for example, by presenting a card to a terminal). Transactions in quick service restaurants, at kiosks or vending machines and at transit locations are expected to be very fast, with a card simply being waved at the terminal. A card that will be used in multiple environments must be appropriate for the worst-case scenario.

Key technical characteristics include operational range, operational orientation, time in field, anti-tear and anti-collision capabilities and supported form factors.

Operational range is determined by system design and limited by standards, regulations, or technology characteristics. It may be important for the card to be placed close enough to the reader to signal an intentional payment act by the consumer. At longer operational ranges, there is a perceived risk (and potentially a real threat) that a fraudulent or inadvertent transaction could be executed. For certain applications, like parking and drive-through restaurants, this risk may be acceptable, given that short ranges may not provide an acceptable user experience. RF-based systems typically offer a very good user experience because they are quite forgiving in terms of how close the card must be to the reader.

Flexibility in **operational orientation** can be critical to ease of use. Magnetic stripe cards and contact smart cards must be oriented and inserted or swiped in a particular way. Other payment technologies, like IR, require that the card be pointed in a particular direction. Contactless smart cards do not have to be oriented or moved in a particular way during a transaction (depending on the operational range). This flexibility has significant advantages for throughput, reduction of repetitive actions, and increased customer satisfaction.

Time in field depends on system design and technology characteristics such as range, amount of data required to complete a transaction, data rates, and operational conditions (e.g., error rate due to interference). Higher frequencies and data rates may be essential to ensure adequate bandwidth for effective security. Real transactions must be tested thoroughly to ensure that the time in field meets consumer expectations and operational goals. Transaction types incorporating significant data exchanges must balance performance, security, and processing overhead. Contactless transactions are as much about ergonomics and environment as they are about transaction integrity. Typical "high flow" transit applications, for example, may require transactions to be completed in less than 150 to 300 milliseconds.

Smart Card Alliance © 2003

Anti-tear provisions are extremely important in "high flow" environments (e.g., transit) where data is being processed and then updated on the card. The card and application must be able to prevent incomplete transactions and corruption of card files by early removal of the card from the communications field.

Anti-collision is unique to contactless technologies since more than one card can be placed in the communications field at the same time. Product features must be in place to "sort out" the prioritization of devices in the communications field. The ISO/IEC 14443 and ISO/IEC 15693 standards specify how anti-collision is handled.

Device **form factor** (e.g., card, key fob, watch) is an important consideration for both the user and the service provider. Users want form factors with which they are comfortable or which are convenient and complete transactions quickly. The service provider needs form factors that will meet operational goals (for example, throughput requirements), boost customer loyalty and acceptance, and be secure and reliable.

Commercial Availability

Appropriate technology should be selected based on commercial availability and on whether the technology has a demonstrated capability to support payment applications similar to those being considered. Standards-compliant systems are generally a better choice: there are typically more sources for components, the technology has undergone more independent scrutiny and, over time, economies of scale drive costs down.

It is important to understand the complete cost of ownership for any technology. For example, using a card form factor allows for very cost-effective and automated branding, personalization, fulfillment, and integration into existing customer relationship management (CRM) systems.

Required Investment

Two major factors affect the amount of investment required to implement a payment system using a particular technology: the system architecture and the selected payment type. The amount of required investment depends first on whether the retailer buys into an existing network, builds a system based on an open architecture, or builds a proprietary solution. The chosen payment type may dictate additional investment in at least three major areas: POS upgrades, transaction processing infrastructure, and supporting systems (e.g., customer support). The next section, "Contactless Payment Transaction Models," summarizes the requirements for each payment type.

In general, the amount of investment required depends on what type of systems the retailer currently has in place, whether there are multiple vendors for the selected devices and POS terminals, and what the costs are for connecting to a particular network. Depending on the issuer model (for example, retailers may elect to issue their own cards), significant additional costs could be associated with acquiring new customers or supplying existing customers with payment devices.

Merchant transaction processing requirements will also affect infrastructure costs. For example, using EMV in North America will be more costly than using other approaches. Card-based contactless payment systems have an

edge over other form factor and technology choices. Their rapid adoption for transit applications has resulted in increased availability of standards-compliant off-the-shelf components and systems from a growing number of vendors. Publicly funded transit infrastructure also provides a nucleus from which non-transit initiatives can build in key geographic areas.

Risks and Security

To evaluate the risks introduced by contactless payment, it is necessary to understand the differences between current and proposed payment systems. For example, it is generally known that magnetic stripe cards are susceptible to fraud and that smart cards with appropriate security technology can significantly mitigate this risk.

Contactless technology does not typically introduce additional points at which a system is potentially vulnerable, with the exception of the air interface between the consumer payment device and the POS terminal. Appropriate token-to-reader authentication and data security services significantly reduce this vulnerability. Contactless smart card solutions are available today that have stronger security than magnetic stripe cards and also reduce the losses and costs inherent in paying with cash or by check. If lower cost and less powerful contactless devices are selected, it is important to understand any inherent potential threats and ensure that appropriate safeguards are adopted.

As is true for any system upgrade, a system security analysis should be conducted, since changes in transaction flow and processing and human interaction can introduce new vulnerabilities. Understanding these risks will also help determine what fees apply to any contactless transactions.

Figures 2 and 3 summarize the key technical specification and business factors that may be considered in selecting the contactless technology to deploy for a payment system.

	ISO/IEC 14443	ISO/IEC 15693	Proprietary 13.56 MHz	Low-frequency RF	Ultra-high-frequency RF	Infrared (Lightwave)	Bluetooth (Microwave)
Operational range	<10 cm	<70 cm	<10 cm	<20-60 cm	3.5 to 10+ m	1-2 m; 20-30 cm with low power	10 - ~80 m
Operational orientation	Within RF range, depending on antenna	Within RF range, depending on antenna	Within RF range, depending on antenna	Within RF range, depending on antenna	Within restricted antenna beam	Line of sight only, with accurate alignment required	Wide range but potential conflict with multiple devices
Data rates	106-424 Kbps	26 Kbps	FeliCa: 211 Kbps GO CARD: 115-460 Kbps	<10 Kbps	20-100 Kbps	9.6 Kbps to 4 Mbps	1 Mbps
Carrier frequency	13.56 MHz	13.56 MHz	13.56 MHz	100-300 KHz	902-928 MHz	Not applicable	2.4 GHz ISM band
Standards-based communi-cations link	ISO/IEC 14443 Types A/B	ISO/IEC 15693	No	No	Most are proprietary; no single global standard	Specified under auspices of the IrDA trade association (IrFM)	Specified under auspices of the Bluetooth trade association
Standards-based payment protocol	Visa: EMV MasterCard: Track 1 and 2 magnetic stripe data JCB	No	FeliCa: JCB GO CARD: None	No	No	Visa: Refers to IrFM 1.0 and adds security and other requirements	No
Availability of POS terminals	Multiple vendors	Multiple vendors	FeliCa: Multiple vendors GO CARD: Cubic	Multiple vendors	Available for trials	Available for trials	Available for trials
Security	Perceived security advantage due to intentionality of payment due to short range; more capable, crypto-enabled proc-essors; wired logic security services	Can operate at either long or short ranges; wired logic security services	Perceived security advantage due to intentionality of payment due to short range; more capable proc-essors or wired logic security services	Typically transactions are short range; less capable proc-essors and low data rates	Perceived security threat due to longer range; much less capable processors	Low-level security via line of sight with 30° cone; application level security required for higher strength (e.g., as specified by Visa)	Strong authentication must be built into application
Available form factors	Plastic card Watch Mobile phone	Plastic card Watch Key fob	Plastic card	Plastic card Key fob Watch Car tag Mobile phone	Car tag	Any IR-capable device	Any Bluetooth-capable device

Figure 2: Contactless Technology Comparison: Technical Features

Smart Card Alliance © 2003

1608

Figure 3: Contactless Technology Comparison: Business Issues

	ISO/IEC 14443	ISO/IEC 15693	Proprietary 13.56MHz[41]	Low- frequency RF	Ultra-high-frequency RF
Availability in card form factor	Yes	Yes	Yes	Yes	No
Payment association support for payment	MasterCard, Visa, JCB	No	FeliCa: JCB GO CARD: None	No	No
Current market deployment for retail payment applications	Extensive worldwide, with over 200 million cards used in transit AFC; trials in US	Not historically used for payment	FeliCa: Extensive worldwide for AFC; 25 million shipped world-wide GO CARD: Selected in major cities in North America for AFC	Over 6 million Speedpass activated fobs, plus several other trials in the U.S.	Trials in the U.S. for retail payment
Availability of cards/ tokens and readers	Many vendors	Multiple vendors	FeliCa: Multiple vendors for cards and readers GO CARD: Multiple vendors licensed by Cubic for cards; Cubic for readers	Typically single source per proprietary implementation, though multiple vendors provide technology	Few vendors
Integration with payment processing services	MasterCard trial in U.S.; Visa trials in Asia that link to existing credit networks; AFC	Bank of America QuickWave pilot; Shell Canada	JCB in Japan with Kansai Thru Pass; AFC and parking	Typically pre-authorized account-based proprietary infra-structure con-necting to exist-ing financial networks (e.g., Speedpass)	Typically pre-authorized account-based proprietary infrastructure connecting to existing financial networks
Inter-operability	Potentially strong – based on standards, with Visa endorsing contactless pay-ment standard	Potentially strong – based on standards	Non-standard technology; like technologies are interoperable.[42]	Weak since based on proprietary systems	Weak since based on proprietary systems
Ease of use by consumer	Strong. Variety of form factors, but shorter oper-ational range	Strong. Variety of form factors, with longer potential operational range	Strong. Variety of form factors, but shorter oper-ational range	Strong. Variety of form factors, with longer potential oper-ational range	Strong. Variety of form factors, with longer oper-ational range
Ease of integration with mer-chant POS terminals	Easy, with addition of adapter	Easy, with addition of adapter	Easy, with addition of adapter	Easy, with addition of adapter	More difficult due to antenna size

[41] Data shown is for Sony FeliCa technology and Cubic GO CARD technology.
[42] In North America, the American Public Transportation Association (APTA) is working on interoperability specifications for transit applications.

Contactless Payment Transaction Models

The transaction model for contactless payment applications varies depending on the implementation approach. This section describes the end-to-end transaction model for the following contactless payment application implementations:

- Speedpass
- E-ZPass
- Payment using Track 1 and Track 2 data on a contactless smart card
- EMV credit/debit card
- Offline stored value card

The activities of the consumer, retailer, acquiring processor, and issuing bank are summarized for each application, as is the expected retailer investment. The descriptions assume that the retailer currently supports credit card transactions, where the credit cardholder data is received by swiping a magnetic stripe credit card at the POS.

Speedpass

Speedpass as used at a gas pump is implemented as a pre-authorized account-based payment, authorized on a transaction-by-transaction basis. The table below summarizes the process that takes place when consumers use Speedpass at a gas pump. The Speedpass system uses a low-frequency RFID payment device that identifies the consumer and processes the transaction as a traditional credit or debit card transaction.

Step	Consumer	Retailer/ Service	Acquiring Processor	Issuing Bank
1	The consumer waves the Speedpass key tag in front of the sensor (1 - 2 inches away).			
2		The sensor on the pump senses the tag. The contactless reader in the pump reads the information from the tag and the sensor lights up.		
3		The information read from the Speedpass key tag (Speedpass ID/serial number) is sent to the Speedpass central database for authentication.		
4			The bank card information tied to the Speedpass tag is retrieved.	
5			The bank card data and request for authorization are transmitted to the bank issuing the card.	

Step	Consumer	Retailer/ Service	Acquiring Processor	Issuing Bank
6				The issuing bank authorizes or denies the transaction.
7		The issuer's response indicates whether the consumer can pump gas. If the request is denied, the pump is not enabled and the process terminates with the Speedpass light going off.		
8	The consumer selects a grade of gas and pumps the gas.			
9		The cost of the sale is computed at the pump and the amount is transmitted back to the processor.		
10			The transaction amount is forwarded to the issuing bank.	
11				The amount is entered as a charge to the consumer's corresponding bank card account.
12		A receipt is issued at the pump. The sale data are entered in the gas station's electronic ledger. The pump returns to the idle state.		
13	The consumer takes the receipt and the transaction is complete.			

A retailer who wants to accept payment using Speedpass technology requires the following infrastructure:

- POS terminals enabled with devices that can communicate with the Speedpass RFID key tags.
- A POS application that can format the authentication message to be sent to the Speedpass server for authorization and settlement.
- POS systems that can establish a connection with the server hosting the data that translates the Speedpass key tag ID to a credit card number.

E-ZPass

E-ZPass is implemented as pre-authorized account-based payment with set transaction limits. E-ZPass uses an ultra-high-frequency RFID payment device that identifies the consumer to a central system in which the consumer's account and transaction limit information is stored. The consumer funds and replenishes the account using traditional payment methods. The table below summarizes the payment process that takes place when consumers use E-ZPass.

Step	Consumer	Retailer/ Service	Acquiring Processor	Issuing Bank
1	The consumer approaches the toll lane. The E-ZPass tag sends out a radio signal with the consumer's E-ZPass account information.			
2		The E-ZPass information is read by a receiver above the lane.		
3		The E-ZPass information is decoded and sent to the E-ZPass central database.		
4			The E-ZPass information is processed and the appropriate amount is deducted from the consumer's pre-paid account (funded from the consumer's credit or debit account).	
5		If the transaction is successful, the light at the toll lane turns green.		
6	The vehicle passes through the tolls without stopping since the transaction takes only a fraction of a second.			

A retailer who wants to accept payment using E-ZPass technology requires the following infrastructure:

- POS terminals enabled with devices that can communicate with the E-ZPass transponder.
- A POS application that can format the data to be sent to the E-ZPass server for authentication and settlement.
- POS systems that can establish a connection with the servers on which details about the E-ZPass accounts are stored.

Contactless Payment Using Track 1 and Track 2 Magnetic Stripe Credit Card Data

Consumers can use a contactless payment card that transmits Track 1 and Track 2 magnetic stripe credit card data to retailer POS systems. The transaction is then processed as a traditional credit or debit card payment. Data included on Track 1 and Track 2 identify the cardholder by cardholder name, card number, and expiration date; this information is stored in the contactless smart card chip when the card is issued. The MasterCard U.S. pilot uses this transaction model, implemented using ISO/IEC 14443 contactless smart card technology. The table below summarizes the

payment process that takes place when consumers use a contactless card with Track 1 and Track 2 data.

Step	Consumer	Retailer/ Service	Acquiring Processor	Issuing Bank
1	The consumer presents the card to the contactless reader.			
2		The contactless reader exchanges data with the card. The POS terminal now "knows" the card-holder magnetic stripe data.		
3		The POS application gathers the data and the dollar amount of the transaction and creates an authorization request for the acquiring processor.		
4			The request for authorization and credit card data are transmitted to the financial institution issuing the credit card.	
5				The issuing bank authorizes or denies the transaction.
6		The issuer's response indicates whether the consumer can complete the purchase.		
7	If the transaction was authorized, the consumer takes the receipt and signs a copy for the merchant. The transaction is complete.[43]			

A retailer who wants to accept payment using data from a contactless version of a traditional credit/debit card requires the following infrastructure:

- POS terminals enabled with devices that can communicate with the contactless credit cards to receive Track 1 and Track 2 data.
- A POS application that can receive credit card data by means of a contactless interface. In the MasterCard PayPass pilot, no application software change is required if using a special retrofit adapter.[44]
- The authorization and the settlement mechanism are the same as when using a magnetic stripe card for payment.

[43] In some cases, a consumer signature may not be required.

[44] "Contactless POS Environment," presentation by Mohammad Khan, ViVOtech, Smart Card Alliance Mid-Winter Conference, February 12, 2003.

Contactless Credit/Debit Card Using EMV

The table below summarizes the payment process that takes place when consumers use a contactless smart card for EMV credit and debit transactions.

Step	Consumer	Retailer/ Service	Acquiring Processor	Issuing Bank
1	The cardholder selects goods and presents an EMV credit/debit card.			
2		The EMV card and the EMV terminal perform risk management functions. The card signs the transaction data. The terminal sends the purchase price, card data and signed data for authorization.		
3			The acquirer forwards the transaction data to the issuing bank for authorization.	
4				The issuer verifies the signed data to prove the transaction came from a legitimate card and authorizes or denies the payment. If the payment is authorized, the issuer debits the cardholder's account.
5			Authorization or denial is received from the issuer and is returned to the retailer.	
6		The issuer's response is received and stored. If the transaction is authorized, goods are sold to cardholder.		
7	If the transaction was authorized, the consumer takes the receipt and signs a copy for the merchant. The transaction is complete.[45]			

A retailer who wants to accept payment using contactless EMV technology requires the following infrastructure:

- POS terminals enabled with devices that can communicate with EMV credit/debit cards by means of the contactless interface and receive the EMV data personalized on the card. The POS terminal hardware used must be EMV Level 1 and Level 2 certified.
- A POS application that receives EMV data by means of a contactless interface and supports the authorization and settlement of an EMV

[45] In some cases, a consumer signature may not be required.

transaction. This may require changes to other POS systems and changes to the connection to the retailer's payment processor.

Additional information on the infrastructure required to support EMV payment can be found in the Smart Card Alliance white paper "Smart Cards and the Retail Payments Infrastructure: Status, Drivers and Directions."

Stored Value Card

Contactless offline stored-value cards hold a monetary value for use by a consumer. The table below summarizes an example process that allows consumers to use an offline stored-value card for payment.

Step	Consumer	Retailer/ Service	Acquiring Processor	Issuing Bank
1	The cardholder makes a purchase.			
2		The amount of purchase is encrypted and requested from the card.		
3	The card receives and authenticates the request, debits the internal value, and encrypts and sends the purchase value to the retailer.			
4		The retailer receives the value and stores the payment locally.		
5		The retailer sends a batch of all sales (values received) to the processor.		
6			The batch is checked and passed on.	
7				The issuer checks the batch and credits the retailer account.
8			A confirmation message is routed to the originator.	
9		The retailer receives confirmation of payment.		

A retailer who wants to accept payment from a stored value card requires the following infrastructure:

- POS terminals enabled with a device that can communicate with the contactless stored value cards.
- A POS application that supports a stored value transaction according to the scheme selected for stored value payment. The stored value application must also implement the authorization and settlement process for the stored value transaction.

Why Contactless Smart Cards?

As payment mechanisms, credit and debit cards are now ubiquitous. The usual question from most retailers to a customer who wants to make a purchase is "How do you want to pay?" meaning "Do you want to pay using cash or using a credit or debit card?" The payment card technology used by the banking industry is now evolving from the traditional magnetic stripe card technology to smart card technology in many regions of the world, with varying rates of introduction depending on business requirements for added functionality or higher security.

This section summarizes the advantages of contact and contactless smart cards as compared to other current payment mechanisms.

Why Smart Cards?

The use of smart card technology is helping the payments industry and associated markets develop new business opportunities. The smart card's expanded memory and processing capabilities permit multiple payment and non-payment applications on a single card, with features that both ensure security and enhance privacy. Smart card technology is also ideally suited for Internet and e-commerce transactions.

Application Flexibility

With magnetic stripe cards having limited memory, smart card technology provides the flexibility and capacity for new applications that can drive both retailer and issuer business cases. Opportunities are now available to develop partnerships to handle multiple functions with a single card (such as a payment card linked to a retailer loyalty scheme) or to develop true independent applications and combine multiple applications on a single card (using frameworks such as Visa's Global Platform or MasterCard's MultOS™). New applications (for example, a retailer loyalty program) can now be issued during the life of the card, expanding card services. Increasingly, card issuers and retailers are exploring a range of new and innovative business cases that will help to provide competitive differentiation.

The payment solution need not necessarily be credit or debit; it could be (for example) a closed system electronic purse linked to a mass transit scheme, or a solution linked to a Visa, MasterCard, American Express or JCB brand. The more versatile the card, the more likely it is to be accepted by users. American Express has reported that 67% of their cardholders said they would charge less to their Blue card if there were no chip in the card,[48] indicating that smart cards are already finding user acceptance in the United States.

Security

Smart cards were originally developed to address security issues and they continue to provide a highly secure solution for numerous applications (e.g., payment, identity verification for physical and logical access, data storage).

[48] "TowerGroup Offers Rosy Forecast for Chips in U.S., *American Banker*, January 29, 2002.

As an example, in the late 1970s, G.I.E. Cartes Bancaires demanded a bank card offering superior protection and significantly improved security against fraud to counteract an escalating level of fraud in France. The solution, conceived by Bull Information Systems, was to add intelligence to the card by embedding a microprocessor that would react intelligently to information received and protect data stored in memory. Smart card payment that is based on the EMV (Europay MasterCard Visa) specification is now being deployed in Europe, Latin America and Asia to reduce credit card fraud and telecommunications expense.

Smart cards provide strong security capabilities for all applications supported by a card. Security features include:

- Large memory size that can support the addition of software providing enhanced security features or new applications.
- Extreme difficulty of replication. The difficulty of obtaining a source for chips that have been manufactured with specific embedded software, coupled with the difficulty of reading data encrypted in chips, provide significant barriers to counterfeiting cards. The widespread practice of skimming and producing "white cards" is not practical with smart cards.
- Enhanced decision-making process with the card reader. Smart cards support both online and offline card verification and the use of strong encryption algorithms. Smart cards can therefore provide better protection and security for transactions at unattended terminals.
- Strong identity verification features. For example, the use of a PIN rather than a signature with a smart card may significantly reduce the opportunities for fraud. A smart card can also include biometric data (such as a digitized photograph, fingerprint, iris scan, or voice print) to enhance security. Although biometrics are not yet widely used for identification in the payment industry, they are starting to be used by applications such as personal identification confirmation and access control.
- Ability to meet specific market requirements and evolve as requirements change (for example, adding additional risk management features that are needed for transaction processing models in some markets).

While smart cards cannot solve all transaction security issues (for example, "'card not present" transactions), they provide an excellent solution that delivers a high degree of security, along with application flexibility and growth. This is particularly important in the United States where fraud rates are low (since the majority of payment transactions in the United States are authorized online and issuers are using sophisticated fraud detection tools and neural networks to identify fraud). As a result, it is expected that the driving business case for smart cards in the United States will be based on revenue generation, new payment types and value-added applications.

Why Contactless?

The primary advantages to both the consumer and retailer of using any contactless technology for payment applications are convenience and speed. Convenience comes primarily as a result of speed: no fumbling for exact change while getting on a bus with parcels or while standing at the checkout counter, and no delay to put a ticket or card into a mechanical reader with the proper orientation when rushing to catch a train. The option of not needing to remove the card from a wallet or handbag, but merely needing to pass the

wallet or bag within a few centimeters of the reader, provides additional convenience.

For the retailer, contactless technology also means more rapid throughput, resulting in fewer queues and smaller numbers of checkout staff. Initial results from MasterCard's PayPass pilot showed that PayPass reduced transaction times by up to 64%. Mass transit authorities show increased throughput of from 15 - 20% (according to Hong Kong's Octopus card statistics).

Contactless technology is an ideal payment method for unattended terminals, such as vending machines, toll booths, gas stations, transit stations and parking meters, especially in potentially dirty or harsh environments (such as exterior parking lots, gas stations, or toll booths). The absence of coins decreases opportunities for using fake coins or vandalizing the machines used to collect payment by damaging or blocking coin or card slots. Contactless technology implementations also have higher reliability (with fewer components to maintain), leading to increased availability and decreased maintenance costs.

In those regions where mass transit is using contactless smart cards for payment, it is also feasible for interested third parties to team with regional transit operators and form commercial alliances aimed at sharing costs and generating value.

Global Standards

The importance of standardization to mass acceptance of a new method of payment cannot be overstated. The presence of international and industry standards helps ensure that systems are reliable, that components can be manufactured correctly, and that there is a choice of vendors. The smart card industry has developed standards for both contact and contactless cards and terminals.

There are four key standards:

- ISO/IEC 7816 for smart cards.
- ISO/IEC 14443 for contactless proximity cards.
- ISO/IEC 15693 for contactless vicinity cards.
- EMV 2000 for payment cards.

For more information on these standards, refer to the Smart Card Alliance reports "Smart Cards and the Retail Payments Infrastructure: Status, Drivers and Directions" and "Contactless Technology for Secure Physical Access: Technology and Standard Choices."

Why Contactless Smart Cards for Payment?

Cards are the dominant form factor used for payment. Consumers are comfortable and familiar with using a card for payment. The fact that a traditional magnetic stripe payment card has evolved into a chip-based contactless smart card that can be waved by a reader makes the new payment device even easier to use. The additional security provided by the smart card also provides greater comfort to consumers who are increasingly aware of the risk of card fraud and identity theft. By providing a payment

device that is familiar and that can be used at a wide variety of retailers, issuers can increase its acceptance and usage.

Datamonitor estimates that contactless smart cards across all applications (e.g., payment, transit, access) will grow from approximately 100 million cards in 2002 to 280 million in 2006. Although conventional contact smart cards still represent more than 95 percent of the $42.3 billion smart card market in 2002, the market for contactless cards is growing at twice the rate of contact smart cards.[47]

The benefits of using contactless smart cards for payment applications can be summarized as follows:

- Increased security.
- The flexibility to develop product partnerships and differentiators.
- Greater consumer convenience.
- Increased throughput for high-volume traffic.
- Potentially lower staffing costs.
- Greater reliability for reader terminals.
- Lower maintenance cost for reader terminals.
- Longer card life due to no mechanical wear from reader insertion.
- Longer life for unattended terminals.
- Support from all payment associations.
- Potential synergies with local transit agencies.
- Global industry standards to ensure the availability of the required product.

Visa, MasterCard and JCB have all launched programs based on contactless smart card technology. The recent announcement of MasterCard's PayPass trial states that 63% of the consumers surveyed said they would "definitely" or "probably" use PayPass if their bank offered it to them. Achieving such percentages would clearly indicate that the contactless smart card provides a desirable payment option.

[47] *Card Technology*, October 2002, op. cit.

Conclusion

An increasing number of payment applications worldwide are using contactless technology. Such applications range from automatic fare collection systems to retailer acceptance of transit payment methods to payment systems that use the existing credit and debit payment infrastructure. The benefits of contactless payment for the consumer and retailer have been proven in numerous implementations. Increased convenience for the consumer has resulted in increased sales and faster transaction times for the retailer. The retailer also has lower costs due to fewer requirements to handle cash, improved operational efficiencies, and lower maintenance costs resulting from improved reliability of card readers.

Although interest in contactless payment is growing, currently no single technology is being used for contactless payment in the United States. Several technologies are now vying to become the solution of choice for retailers. Both contactless smart cards and ultra-high- and low-frequency RFID have been used in a number of implementations. It is also possible that future solutions could be based on IR, Bluetooth, Near Field Communication, and carrier-based mobile technologies. The contactless payment process also varies, depending on the solution, with some solutions using a traditional credit/debit card transaction and others implementing a unique closed-system approach.

Retailers who would benefit from the speed and increased convenience of contactless payment should evaluate the different technologies and assess which best meets both short- and long-term requirements for their payment processes. Important factors to the retailer's choice include payment device issuance and management processes, integration with current payment and business processes, availability of necessary system components, and long-term stability of the technology, products, and services.

Contactless smart card-based systems offer an excellent choice for retailers. Contactless smart card technology is based on international standards and has been proven in implementations worldwide. Smart cards are being used for payment throughout the world, with Visa, MasterCard and JCB leading initiatives to extend the use of smart cards for contactless payment. In addition, large-scale implementations of smart card-based transit payment systems are scheduled for a number of major cities in the United States in the next 18 to 24 months. The combination of standards-based technology, extensive security features, availability of products and services from multiple vendors, potential to use the existing payments infrastructure, and support from major financial industry players offer compelling benefits for contactless payment implementations based on smart cards.

Retailers can create a strategic competitive advantage and increase sales by accepting new forms of payment. The Smart Card Alliance urges retailers to evaluate the benefits of implementing contactless payment and to consider smart card-based solutions.

For more information about smart cards and the role that they play in retail payment and other applications, please visit the Smart Card Alliance web site at www.smartcardalliance.org or contact the Smart Card Alliance directly at 1-800-556-6828.

References and Resources

"Access Will Overtake Transit as Contactless Card Application," *Card Technology*, October 2002, page 25.

American Public Transport Association (APTA), http://www.apta.com

Bluetooth Consortium, http://www.bluetooth.org/

"Consumer Payment Systems," *The Nilson Report*, Issue #777, December 2002.

"Contactless POS Environment," presentation by Mohammad Khan, ViVOtech, Smart Card Alliance Mid-Winter Conference, February 12, 2003.

"Contactless Smart Card Schemes in the Asia Pacific Region," Asia Pacific Smart Card Association report, August 2002.

"Contactless Smart Card Technology for Physical Access Control," Avisian, Inc., April 1, 2002.

"Contactless Technology for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance, October 2002.

Amy Cortese, "Tollbooth Technology Meets the Checkout Lane," *New York Times*, July 7, 2002.

"Cubic Receives Contract to Integrate Smart Card Technology into Houston METRO's Fare Collection System," Business Wire, December 13, 2001.

Donald Davis, "The Contactless Wave," *Card Technology*, January 2003.

"Easing Travel in London's congested public transport network," *On the Move Identification News,* July 2002.

John Elliott, "Losing contact: the transactions of the future are disappearing into thin air," *Cards Worldwide*, March 15, 2002.

John Frank, "Visa selects ISO 14443 as its standard for global contactless payments," *ContactlessNews*, December 2002.

"Gilbarco Wants to Help Gas Stations Pump Up Profits," *RFID Journal*, June 2002.

Hong Kong Octopus Cards web site, http://www.octopuscards.com

Infrared Data Association, (http://www.irda.org). Includes an IrDA comparison of IR with Bluetooth at http://www.irda.org/design/irdavbluetooth.htm

Intelligent Transportation Society of America (ITSA), http://www.itsa.org/payment.html

Jon Karlen, "Contactless Micropayments," *Wireless Future Magazine*, September/October 2002.

Edward Kountz, "RFID Payment Fobs at Point of Sale: The Early Face of M-Payments in North America," TowerGroup, March 2002.

MasterCard PayPass web site, http://www.paypass.com

Matthew Miller, "Received Wisdom," *CommVerge*, Nov. 1, 2002.

"Mobil Speedpass Goes Global as Mobil Singapore Rolls Out Asia's First RFID-Based Pay-At-The-Pump System," Texas Instruments press release, April 5, 1999.

Mobile Payment Forum, http://www.mobilepaymentforum.org

"New MasterCard PayPass Utilizes Contactless Payment Technology," MasterCard press release, December 12, 2002.

"Philips and Sony Announce Strategic Cooperation to Define Next Generation Near Field Radio-Frequency Communications," Philips press release, September 5, 2002.

"The Public Sector Takes the Lead," *Card Management*, February 2002.

"San Francisco's Transit Smart Card Pilot Grows," *Card Technology News Bulletin*, June 12, 2002.

"Smart Cards: Seizing Strategic Business Opportunities," Smart Card Forum, edited by Catherine A. Allen and William J. Barr, McGraw-Hill, 1997

"Smart Cards and the Retail Payments Infrastructure: Status, Drivers and Directions," Smart Card Alliance white paper, October 2002.

Speedpass web site, http://www.speedpass.com

"Timex Watch Offers Convenience of Speedpass Technology with the Wave of Your Wrist," *Texas Instruments RFID eNews,* Issue No. 14, November/December 2002.

"Toronto Transit Jumps on the Smart Card Bandwagon," Card Technology News Bulletin, July 3, 2002.

"TowerGroup Offers Rosy Forecast for Chips in U.S., *American Banker*, January 29, 2002.

"A tube full of oysters? London goes contactless..." *ContactlessNews*, December 2002.

"U.S. Smart Card Breakthrough," The Nilson Report, January 2003.

"Visa, MasterCard diverge on proximity payments," *European Card Review*, August 2002.

Visa Financial Messaging Profile for Contactless Payment, http://www.corporate.visa.com/mc/press/press112.html

Publication Acknowledgements

This report was developed by the Smart Card Alliance to discuss contactless payment technologies and applications. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Secure Personal ID Task Force members for their comments and contributions. Members from 23 organizations, both public and private, were involved in the development of this report including: ASSA ABLOY ITG; Atmel; Citicorp EFS; Cubic; EDS; ERG Group/Proton World; First Data; Hypercom; IBM; JCB International Credit Card Co.; MartSoft Corporation; MasterCard International; NTRU Cryptosystems, Inc.; Oberthur; Philips Semiconductors; Potomac Systems and Technologies; SchlumbergerSema; Smart Commerce Inc.; Office of the Comptroller of the Currency; Visa International; Visa U.S.A.; ViVOtech; WMATA.

Special thanks go to the Task Force members who wrote, reviewed and edited this report.

Manuel Albers, Philips Semiconductors
Dovell Bonnett, ASSA ABLOY ITG
Matt Byrne, First Data
Dan Cunningham, Potomac Systems and Technologies
David deKozan, Cubic
Amol Deshmukh, SchlumbergerSema
Ian Duthie, Atmel
Greg Garback, WMATA
Kim Gregory, Cubic
Mick Hosken, Visa International
Mansour Karimzadeh, Smart Commerce Inc.
Diana Knox, Visa U.S.A
Julie Krueger, JCB International Credit Card Co.
Michael Madden, MasterCard International
Cathy Medich, Consultant and Task Force Chair
Joe Pilozzi, Philips Semiconductors
Carlos Rachedi, ERG Group/ Proton World
Jim Russell, MasterCard International
Randy Vanderhoof, Smart Card Alliance
Cliff Wilke, Office of the Comptroller of the Currency
Jeremy Wyant, NTRU Cryptosystems, Inc.

Copyright Notice

Copyright 2003 Smart Card Alliance, Inc. All rights reserved.

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.

Appendix A: Contactless Transit Implementations

Mass transit agencies have been using stored value pre-payment cards for electronic ticketing since the early 1970s. Through the 1990s this segment steadily began transitioning from magnetic stripe technology to contactless smart cards for a variety of operational and user convenience reasons. This led to large-scale investments in standards and product development by the semiconductor and card manufacturing communities. Today, virtually all new transit fare payment systems either in the delivery or procurement stages involve the use of contactless smart cards as the primary ticket media. Already, major deployments are up and operational in a variety of cities including Hong Kong, Seoul, Pusan, Washington DC, and Shanghai.

Over the course of 2003 and 2004, a number of major cities across the United States and Europe will be rolling out large-scale contactless smart card deployments for mass transit. These include London, Los Angeles, Chicago, San Diego, Minneapolis, Houston, San Francisco, and the expansion of the Washington DC program to include all of northern Virginia and the entire state of Maryland.

Transit communities are deploying this technology to establish integrated fare solutions across a broad regional geography and multiple modes of transport (including rail, bus, transit van, and ferry). Many are being extended to include parking and access control applications.

Many countries are in the midst of establishing interoperability standards, which will govern the application file record contents, access conventions, communications protocols, and inter-system messaging conventions. Examples include ITSO in the United Kingdom, VDV in Germany, and the Universal Farecard Standards Task Force working under the American Public Transportation Association (APTA) in the United States. Universally, these standards initiatives reference the ISO/IEC 14443 standard as the basis for card and reader specifications.

The significance of these initiatives extends beyond mass transit as regional fare implementation programs include the broad distribution of smart card terminals across concentrated geographies. Transit ridership profiles also extend over all segments of regional demographics since most people who live in major metropolitan areas (particularly those with rail service) use public transit. As such, mass transit is serving to establish both a broadly distributed card base and a broadly distributed infrastructure base. This includes the population of merchant sites with POS terminals capable of processing both contactless smart card and conventional credit and debit payment cards. For example, it is expected that the number of merchants in London, Los Angeles, Washington/Baltimore, Houston and Minneapolis with terminals that accept a contactless transit smart card in addition to other payment cards will grow from 2,300 to over 4,000 over the next 24 months.[48] The introduction of smart card-enabled terminals, particularly in the United States, provides an entry point for new smart card programs aimed at adding other contactless applications.

The following is a list of some of the current or planned North American implementations of contactless smart cards for transit payment. It is not a

[48] Source: Cubic.

complete list. The American Public Transport Association (APTA, www.apta.com) and Intelligent Transportation Society of America (ITSA, www.itsa.org/payment.html) web sites have additional information about smart cards used for payment in North American transit agencies.

- **Atlanta, Georgia**: The Atlanta transit system has issued a request for proposals for an AFC system.
- **Baltimore, Maryland**: The Maryland Transit Administration has awarded a contract for a smart card-based AFC system that will allow riders to pay for travel on bus, subway, light rail and commuter rail systems statewide, using the Washington, DC, area SmartTrip® card. The MTA plans tests in Baltimore in 2003, and implementation by late 2004.
- **Boston, Massachusetts**: The MBTA is in the final stages of a contract award for a new AFC system that includes smart cards, with plans to replace monthly passes and tokens with smart cards by June 2004.[49]
- **Camden County, New Jersey and Philadelphia, Pennsylvania**: The PATCO High-Speed Line is in the design phase of a smart card AFC system to replace a 30-year old magnetic-card system.
- **Chicago, Illinois**: The CTA tested 3,500 smart cards in a pilot in 2000. Issuance of an additional 300,000 cards is expected within 3 years, following the system-wide launch completed in November, 2002.[50]
- **Honolulu, Hawaii**: The city of Honolulu has issued a request for proposals for a smart card-based payment system for the city's bus service.
- **Houston, Texas**: The Houston transit system is upgrading to a smart card-based system.[51]
- **Las Vegas, Nevada**: The Las Vegas monorail will connect seven major casinos to the airport (starting in 2004) and will be based on contactless smart cards.
- **Los Angeles, California**: Implementation of a smart card-enabled infrastructure is underway that will link all public transit (bus, light railway and subway) by 2003.[52]
- **Minneapolis-St. Paul, Minnesota**: Implementation of a smart card-enabled infrastructure is underway with a "smart" regional ticketing system for light rail and bus rapid transit planned by late 2003.[53]
- **Montreal, Quebec, Canada**: The Montreal transit system issued an RFP for AFC modernization.
- **New York, New York**: Plans by the Port Authority of New York New Jersey to rebuild the PATH station destroyed at the World Trade Center include a smart card AFC system that will allow riders to pay fares on buses, subways and PATH.
- **Pittsburgh, Pennsylvania**: The Port Authority of Pittsburgh is planning to use pre-paid contactless smart cards for fare collection for bus and rail networks.
- **San Diego, California**: A joint committee of the county's transit districts has agreed the districts should purchase a smart card AFC system for the area's bus systems.[54]

[49] "The Public Sector Takes the Lead, *Card Management*, February 2002.
[50] Cubic press release, November 27, 2002.
[51] "Cubic Receives Contract to Integrate Smart Card Technology into Houston METRO's Fare Collection System," Business Wire, December 13, 2001.
[52] http://www.mta.net/press/stakeholders/scoop_stories/smart_cards.htm
[53] Cubic press release, January, 18, 2002.

- **San Francisco, California**: The TransLink® system[55] pilot of over 5,000 cards started February 2002, allowing one card to be used for bus, train, light rail or ferry service. Six transportation agencies are using the card (AC Transit, BART, CalTrain, Muni, Santa Clara VTA, and Golden Gate Bus and Ferry Transit).[56]
- **Seattle, Washington**: The Seattle transit system is planning a 2003 implementation of a new contactless AFC system.[57]
- **Toronto, Ontario, Canada**: Go Transit has operated a smart card AFC pilot since July 2001, and plans to extend the program to the Greater Toronto region. A full rollout with issuance of 80,000 cards is expected within 2 years.[58]
- **Ventura County, California**[59]: Ventura County has installed a smart card system on 100 buses, involving 6 public transit operators in the county.
- **Washington, DC**: The Washington Metropolitan Area Transit Authority (WMATA) launched their contactless smart card called SmarTrip in May 1999. With 325,000 cards in circulation, SmarTrip is used for paying fares throughout the Metrorail system and fees at all WMATA-operated parking facilities. WMATA will be expanding the use of SmarTrip to their bus fleet in 2003. Other regional transit operators will become SmarTrip-compatible and included in a unified regional fare payment clearinghouse operated by a third party.

[54] http://www.sdcommute.com/RiderInfo/whatsnew/PDFs/pressreleases/current/02_24a.pdf
[55] http://www.translink.org/jsp/index.jsp
[56] "San Francisco's Transit Smart Card Pilot Grows," *Card Technology News Bulletin*, June 12, 2002.
[57] http://transit.metrokc.gov/prog/smartcard/smartcard.html
[58] "Toronto Transit Jumps on the Smart Card Bandwagon," Card Technology News Bulletin, July 3, 2002.
[59] http://216.103.38.3/sc.htm

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Biometric personal data key (PDK) authentication
First Named Inventor/Applicant Name:	John Giobbi
Filer:	Bowen Zhang
Attorney Docket Number:	

Filed as Large Entity

Filing Fees for ex parte reexam

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
EX PARTE REEXAMINATION (1.510(A)) NON-STREAMLINED	1812	1	12600	12600
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**12600**

Electronic Acknowledgement Receipt	
EFS ID:	45910996
Application Number:	90015053
International Application Number:	
Confirmation Number:	7424
Title of Invention:	Biometric personal data key (PDK) authentication
First Named Inventor/Applicant Name:	John Giobbi
Correspondence Address:	Marissa Ducca - 1300 I Street NW, Suite 900 - Washington, D.C. DC 20005 US - marissaducca@quinnemanuel.com
Filer:	Bowen Zhang
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	08-JUN-2022
Filing Date:	
Time Stamp:	20:10:06
Application Type:	Reexam (Third Party)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$12600

RAM confirmation Number	E202268K11563070
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Receipt of Original Ex Parte Reexam Request	3-905Request.pdf	938110 a055880ac07c71b71c54e6a87843131d142f13e9	no	92
Warnings:					
Information:					
2	Transmittal of New Application	2-905_Transmittal_Form.pdf	200808 2eb0e94ab7f9a4fa69b16cc63ecd53d3d29a4d1c	no	4
Warnings:					
Information:					
3	Reexam - Info Disclosure Statement Filed by 3rd Party	Ex1011-IDS.pdf	222570 346cff7a4602203da0d404d09b7ba2f582b8d5a0	no	2
Warnings:					
Information:					
4	Reexam Certificate of Service	1-905_COS.pdf	127460 68de49cadb0d2f7870e1adff2bce7d887cf729a6	no	2
Warnings:					
Information:					
5	Copy of patent for which reexamination is requested	Ex1001-US9298905.pdf	13514288 4603712551 8c1ebed5ecea4f58642d5c14df2e87	no	15
Warnings:					
Information:					

6	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1002-FH_905_Patent.pdf	20002547 ea8383a9caa0d647c8ed618f9b58d37ba783ec66	no	544
Warnings:					
Information:					
7	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1003-Goldberg_Declaration.pdf	4438002 c95555220561108d78d823c0a4793f29b5179565b	no	182
Warnings:					
Information:					
8	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1004-Goldberg_CV.pdf	78459 6e7f1b0ca826055ca9fea844f32c7eb1a5a0aa7a	no	7
Warnings:					
Information:					
9	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1005-US7188110_r.pdf	4177047 ffbf72ad8e5d3be5d5b2615c125c7f39b916bf0b	no	54
Warnings:					
Information:					
10	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1006-US20030196084A1_Okereke.pdf	7646429 0cd5ab76202e2233c0ee8440d97f71351e6ecd16	no	10
Warnings:					
Information:					
11	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1007-US20030177102A1_Robinson_r.pdf	1989721 5fd59bf9063e85ac11e227a52b0a8f4a2cfd09ff	no	21
Warnings:					
Information:					
12	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1008-WO1999056429A1_Scott_r.pdf	3045838 b066f2c919c2176a139535e2c5e5fc3f6b91be99	no	49
Warnings:					
Information:					

13	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1009-PTAB-IPR2021-01447-12.pdf	385487 972a561444067147e8cb82d9bf42635346b4e593	no	31
Warnings:					
Information:					
14	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1010-Claim_Construction_Order.pdf	182523 8548ac9796d4c8c7f9436940a8b3153f79ab0941	no	5
Warnings:					
Information:					
15	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1012-Introduction_PKI_Kuhn.pdf	572572 07c887f90163c0270998026ee74d7818eecf8578	no	54
Warnings:					
Information:					
16	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1013-Security_Issues_Smart_Cards.pdf	4438786 0dbeb8996415e52d9bc96a1451dd00c035679510	no	6
Warnings:					
Information:					
17	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1014-Smart_Card_Alliance_Web.pdf	471317 517e09380bef1fd69325f3b03edb2a4bf9350954	no	1
Warnings:					
Information:					
18	Reexam - Change in Power Attorney for Third Party Requester	4-905_POA.pdf	91197 77373a56f8cdb545ca609c766f1f53ef566b78a4	no	2
Warnings:					
Information:					
19	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	Ex1015-SCA-2003.pdf	315751 75346996fbba57d8cd704b5ced43c6735c81ccbd	no	50
Warnings:					
Information:					

20	Fee Worksheet (SB06)	fee-info.pdf	37981 69c47d4fd12f6dade622db5f72b0d072aee8184e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	62876893	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: To Be Assigned
Issued: March 29, 2016	Art Unit: To Be Assigned
Application No.: 14/521,982	
Filed: October 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**REQUEST FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Pursuant to 35 U.S.C. § 302 and 37 C.F.R. §§ 1.510 et seq., Samsung Electronics America, Inc. ("Samsung" or "Requestor") requests *ex parte* reexamination of claims 1-18 (the "Challenged Claims") of U.S. Patent No. 9,298,905 ("the '905 patent," Exhibit 1001), entitled "Biometric Personal Data Key (PDK) Authentication." The '905 patent issued on March 29, 2016, from Application No. 14/521,982, which was filed on October 23, 2014.

Patent Owner has asserted the '905 patent against Samsung and Samsung's parent, Samsung Electronics Co., Ltd., in *Proxense, LLC v. Samsung Electronics Co., Ltd., et. al.*, Case No. 6:21-CV-00210-ADA (W.D. Tex.). Because the '905 patent is involved in concurrent litigation, the Patent Office should accord the requested reexamination "priority over all other cases." MPEP § 2261.

TABLE OF CONTENTS

Page

I. INTRODUCTION 19

II. REQUIREMENTS FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510 20

A. Payment of Fees – 37 C.F.R. § 1.510(a) 20

B. Statement Pointing Out Each Substantial New Question of Patentability Based on Prior Art Patents and Printed Publications – 37 C.F.R. § 1.510(b)(1) 21

C. Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art – 37 C.F.R. § 1.510(b)(2) 21

D. Copies of the Cited Prior Art Presented- 37 C.F.R. § 1.510(b)(3) 22

E. Copy of the Patent for Which Reexamination Is Requested- 37 C.F.R. § 1.510(b)(4) 22

F. Certification of Service on the Patent Owner- 37 C.F.R. § 1.510(b)(5) 22

G. Certification of Statutory Estoppel Provisions - 37 C.F.R. § 1.510(b)(6) 23

III. PROCEDURAL HISTORY 23

A. Prosecution History of the '905 Patent 24

B. The IPR filed against the '905 Patent 25

IV. THIS REQUEST SHOULD NOT BE DENIED BASED ON DISCRETIONARY ISSUES 25

V. LEVEL OF SKILL IN THE ART 28

VI. CLAIM CONSTRUCTION 29

A. "third party trusted authority" (claim 1) 30

VII. PRIORITY DATE OF THE '905 PATENT 31

VIII. OVERVIEW OF THE TECHNOLOGY 32

IX. OVERVIEW OF THE PRIOR ART 33

A. Ludtke (Ex. 1005) 33
B. Okereke (Ex. 1006) 35
C. Robinson (Ex. 1007) 36
D. Scott (Ex. 1008) 37
1. A POSITA Would Have Been Motivated to Combine the Teachings of the Ludtke, Okereke, and Robinson 38
2. A POSITA Would Have Been Motivated to Combine the Teachings of Ludtke, Scott, and Robinson 38
X. DETAILED EXPLANATION OF THE PROPOSED REJECTIONS 39
A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1, 3-10, and 12-18 Obvious 40
1. The Proposed Combination 40
(a) The Prior Art Discloses the Claim Limitations 40
(b) A POSITA Would be Motivated to Combine Ludtke and Okereke 42
2. Claim 1 46
(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device" 46
(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;" 49
(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;" 52
(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and 54

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction." 58

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code." 60

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition." 60

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 60

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application." 61

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account." 61

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data." 62

9. Claim 9: 63

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;" 63

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and" 63

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third - party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction." 63

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network." 64

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob." 64

12. Claim 13: 65

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating

that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and" 65

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes." 65

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code." 66

14. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 68

15. Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition." 68

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account." 68

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application." 68

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 2 and 11 Obvious 68

1. The Proposed Combination....68
(a) The Prior Art Discloses the Claim Limitations....68
(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Okereke....69
2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the ID code."....70
3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the ID code....71
C. SNQ 3: Ludtke in combination with Scott Renders Claims 1, 3-10, and 12-18 Obvious....71
1. The Proposed Combination....71
(a) The Prior Art Discloses the Claim Limitations....71
(b) A POSITA Would be Motivated to Combine Ludtke and Scott....74
2. Claim 1....79
(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"....79
(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;"....81
(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"....82
(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and....82

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction." 82

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code." 83

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition." 83

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 83

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application." 83

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account." 84

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data." 84

9. Claim 9: 84

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;" 84

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and" 84

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third - party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction." 85

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network." 85

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob." 85

12. Claim 13: 86

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating

that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and" 86

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes." 86

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code." 87

14. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 87

15. Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition." 87

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account." 88

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application." 88

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 2 and 11 Obvious 88

1. The proposed combination....88
(a) The Prior Art Discloses the Claim Limitations....88
(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Scott....89
2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code. 90
3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the device ID code. 91
XI. REAL PARTIES OF INTEREST 91
XII. CONCLUSION....91

TABLE OF ATTACHMENTS AND EXHIBITS

Attachments

(1) Certificate of Service to Patent Owner
(2) Ex. 1011 Form PTO/SB/08a (Information Disclosure Statement)

Exhibits

The '905 patent, Declaration, and Prosecution History

Ex. 1001	U.S. Patent No. 9,298,905 ("'905 patent")
Ex. 1002	File History of the '905 patent
Ex. 1003	Expert Declaration of Dr. Benjamin Goldberg
Ex. 1004	CV of Dr. Benjamin Goldberg

Prior Art

Ex. 1005	U.S. Patent No. 7,188,110 ("Ludtke")
Ex. 1006	U.S. Patent Publication No. 2003/0196084 ("Okereke")
Ex. 1007	U.S. Patent Publication No. 2003/0177102 ("Robinson")
Ex. 1008	International Publication Number WO 99/56429 ("Scott")

Other

Ex. 1009	Decision Denying Institution of *Inter Partes* Review, Paper No. 12, IPR2021-01447 (February 28, 2022)
Ex. 1010	Claim Construction Order in *Proxense, LLP v. Samsung Electronics Co., Ltd*, Case No. 6:21-CV-00210 (W.D. Tex.) Dkt. 43.
Ex. 1011	Form PTO/SB/08a (Information Disclosure Statement)
Ex. 1012	Introduction to Public Key Technology
Ex. 1013	Security Issues for Contactless Smart Cards
Ex. 1014	Smart Card Alliance Web Site
Ex. 1015	Smart Card Alliance Contactless Payment and the Retail Point of Sale

LISTING OF CLAIMS

CLAIM	LIMITATION
1a	A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device;
1b	responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;
1c	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
1d	responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
1e	responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction.
2	The method of claim 1, further comprising: registering an age verification for the user in association with the ID code.
3	3. The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code.

CLAIM	LIMITATION
4	4. The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.
5	The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.
6	The method of claim 1, wherein completing the financial transaction includes accessing an application.
7	The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.
8a	The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and
8b	responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.

CLAIM	LIMITATION
9a	An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;
9b	a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
9c	a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction.
10	The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.
11	The integrated device of claim 7, wherein an age verification is registered in association with the ID code.
12	The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

CLAIM	LIMITATION
13a	A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and
13b	the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes.
14	The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code.
15	The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.
16	The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal

CLAIM	LIMITATION
	scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.
17	The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.
18	The system of claim 11, wherein completing the financial transaction includes accessing an application.

I. INTRODUCTION

The challenged claims are directed to conventional technology to prevent unauthorized use of a wireless device by verifying both biometric information and the device itself. None of the concepts in the '905 patent were new when the patent was filed; they are clearly disclosed in prior art references that together disclose each and every element of the challenged claims. Moreover, all of the concepts in the patents were used for various different applications for years before the '905 patent was filed. Nevertheless, Patent Owner has launched a lawsuit against Samsung, alleging infringement of technology far newer and more innovative than the technology described in the challenged claims.

The lawsuit against Samsung involves five patents, all relating to similar technology. After the lawsuit against Samsung was filed, Samsung filed IPRs against all five asserted patents. Two of the IPRs were instituted (against US Patent Nos. 9,049,188 and 9,235,700) and are currently pending. The Board denied institution, however, on the '905 patent and two additional related family members: U.S. Patent Nos. 8,352,730 and 10,698,989. In the decisions not to institute the IPRs, the Board found merit in the Patent Owner's argument (which Samsung did not foresee, as it contradicted Patent Owner's claim construction arguments in litigation) that the prior art did not disclose a "third party trusted authority." The

present petition addresses Patent Owner's new argument with different prior art, and therefore presents substantial new questions of patentability.

This Request presents several substantial new questions of patentability. All four SNQs rely primarily on a new reference (Ludtke) that was cited neither during prosecution of either the '905 patent or any of its parents nor in the prior IPR petition regarding the '905 patent. Specifically, SNQ 1 relies on a combination of Ludtke and Okereke, neither of which was presented in the IPR. SNQ 2 relies on a third reference for a single limitation found in a handful of dependent claims. SNQs 3 and 4 rely on a combination of Ludtke and Scott, and while the Scott reference was presented in the IPR, it is cited here only as a secondary reference. Like SNQ 2, SNQ 4 relies on a third reference for a single limitation in a number of dependent claims. Respectfully, these combinations present substantial new questions of patentability that have not been considered by either the PTO or the PTAB.

II. REQUIREMENTS FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510

This request for *ex parte* reexamination of the '905 patent satisfies each requirement of 37 C.F.R. § 1.510.

A. Payment of Fees – 37 C.F.R. § 1.510(a)

Requestor authorizes the Patent and Trademark Office to charge Deposit Account No. DA505708 for the fees set in 37 C.P.R. § 1.20(c)(1) for reexamination.

B. Statement Pointing Out Each Substantial New Question of Patentability Based on Prior Art Patents and Printed Publications – 37 C.F.R. § 1.510(b)(1)

A detailed discussion of pertinent new teachings in the prior art references that present substantial new questions of patentability is provided in Section IX.

C. Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art – 37 C.F.R. § 1.510(b)(2)

Samsung respectfully requests reexamination of claims 1-18 of the '905 patent based on the following proposed rejections:

SNQ 1: Ludtke in combination with Okereke renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 2: Ludtke in combination with Okereke and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 3: Ludtke in combination with Scott renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (b) and (e) and 35 U.S.C. § 103; and

SNQ 4: Ludtke in combination with Scott and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102(a), (b), and (e) and 35 U.S.C. § 103.

A detailed explanation of the pertinence and manner of applying the cited prior art to claims 1-18 of the '905 patent is provided in Section X.

D. Copies of the Cited Prior Art Presented- 37 C.F.R. § 1.510(b)(3)

A copy of every patent or printed publication relied upon as a basis of unpatentability are submitted as exhibits in conjunction with this request for reexamination. In addition, a Form PTO/SB/08a is attached hereto as Exhibit 1011. A full list of exhibits appears on page 11.

E. Copy of the Patent for Which Reexamination Is Requested- 37 C.F.R. § 1.510(b)(4)

A copy of the '905 patent is attached to this Request as Exhibit 1001.

F. Certification of Service on the Patent Owner- 37 C.F.R. § 1.510(b)(5)

The signature on this request certifies that a copy of the request has been served in its entirety on PO's representative at the address provided for in 37 C.F.R. § 1.33(c). Specifically, PO's representative was served by first-class U.S. mail on June 8, 2022, addressed to:

Patent Law Works/Proxense
Greg Sueoka
310 East 4500 South, Suite 400
Salt Lake City, UT 84107

The Requester has also provided courtesy copies to PO's counsel in the aforementioned litigation by first-class U.S. mail on June 8, 2022, addressed to:

Hecht Partners
David Hecht
125 Park Avenue, 25th Floor
New York, NY 10017

Susman Godfrey
Brian Melton
1000 Louisiana St, Suite 5100
Houston, TX 77002

G. Certification of Statutory Estoppel Provisions - 37 C.F.R. § 1.510(b)(6)

Samsung certifies that the statutory estoppel provisions of 35 U.S.C. §§ 315(e)(1) and 325(e)(1) do not prohibit it from filing this ex parte reexamination request.

Requestor previously filed one petition for *inter partes* review against the '905 patent. *See* IPR2021-01447. The petition was denied institution.

III. PROCEDURAL HISTORY

Requestor is unaware of any co-pending Patent Office proceedings involving the '905 patent. This is the first reexamination request challenging the claims of the '905 patent.

The '905 patent claims priority to two provisional patents: U.S. Patent Application Nos. 60/637,538, filed on Dec. 20, 2004, and 60/652,765, filed on Feb. 14, 2005. The '905 patent is a continuation of application no. 13/710,109, filed on Dec. 10, 2012 (now, U.S. Pat. No. 8,886,954), which is a continuation of application no. 11/314,199, filed on Dec. 20, 2005 (now, U.S. Pat. No. 8,352,730). The application that led to the '905 patent was filed on October 23, 2014. The '905 patent issued on March 29, 2016.

A. Prosecution History of the '905 Patent

The '905 patent was filed on October 23, 2014 and claimed the benefit of application no 60/637,538 filed on December, 2004. Ex. 1002 at 482-83, 486.

On June 12, 2015, after lengthy exchange regarding various formalities, the U.S. Patent & Trademark Office (hereinafter "Patent Office") issued the first non-final Office Action rejecting claims 2-18 under 35 U.S.C 103 in light of Hsu et al. (US 6,041,410) in view of Saito et all (US 20040129787) as well as non-statutory double patenting in light of US Patent No. 8,886,954. Ex. 1002 at 94-109.

After amendment and an examiner-initiated interview to suggest terminal disclaimers the Patent Office issued a Notice of Allowance on December 16, 2015. Ex. 1002 at 37-47 and 76-80.

B. The IPR filed against the '905 Patent

Samsung previously filed an IPR against the '905 patent. IPR2021-01447. The IPR presented four grounds. The first two grounds were based on the Scott reference, combined with others. The third ground was based on the Berardi reference in combination with others. The PTAB denied institution of the first two grounds based on its belief that none of the cited prior art disclosed a "third party trusted authority" with respect to claim 1. *See, e.g.*, IPR2021-01447, Paper 12 at 20-26. The PTAB denied institution on the third ground for unrelated reasons. *See, e.g.*, IPR2021-01447, Paper 12 at 27-30.

IV. THIS REQUEST SHOULD NOT BE DENIED BASED ON DISCRETIONARY ISSUES

Patent Owner may argue that this request should be denied in accordance with § 325(d) based on the Federal Circuit's decision in *In re Vivint, Inc.*, 14 F.4th 1342 (Fed. Cir. 2021). That case, however, does not apply here. In *Vivint*, the Requestor filed an *Ex Parte* Reexam request after filing a series of vexatious IPR petitions, the last of which the Board found was an "undesirable, incremental" attack on the Patent Owner. The Board reasoned that allowing such practices "risks harassment of patent owners and frustration of Congress's intent in enacting [the AIA]," and therefore denied the petition. *Id.* at 1346.

Notwithstanding that denial, the Requestor in *Vivint* filed a reexam request that ultimately resulted in cancellation of the challenged claims. On review, the Federal Circuit reversed the CRU's decision to grant the reexam, finding that the request, just like the denied IPR petition, was an abusive filing. The Federal Circuit noted that the vast majority of the reexam was a copy of the denied IPR petition, and the Court concluded that the Director's finding that the IPR petition was abusive should have likewise applied to the reexam request. Specifically, the Court found that the reexam "copied, word-for-word, two grounds from the [denied IPR petition]--the very petition deemed 'a case of undesirable, incremental petitioning.'" *Id.* at 1353. And, for the portions that were not copied, the EPR "used prior Board decisions as a roadmap to correct past deficiencies." *Id.*

The facts here are distinguishable. ***First***, and most importantly, Samsung's previous IPR petition was not a series of "serial" petitions that were "undesirable, incremental petitions." There was only a single prior IPR filed on the '905 patent.

Second, this request is not a "word-for-word" copy of the denied IPR petition. To the contrary, the first SNQ in this request includes *completely new* art that was not seen in either prosecution or the prior IPR. In all four SNQs presented in this reexam, the primary reference, Ludtke, is completely new and was not considered during prosecution or presented in the previously filed IPR. Although

the Scott reference was previously used in the prior IPR, it is used here only as a secondary reference in two SNQs. Similarly, the Robinson reference, which was used for a very specific limitation found in a handful of dependent claims, is also used for that same limitation in the dependent claims. Notably, the Board did not disagree that Robinson teaches that limitation.

Third, this reexam is not using the prior, denied '905 IPR petition as a "roadmap" to correct past deficiencies. In *Vivint*, the requestor copied, word-for-word, two grounds in their entirety, which the Board had already found to be vexatious harassment. Even in the portions that were not copied, the Board found that the same or similar prior art was used. Here, Samsung's request presents entirely new proposed SNQs of rejection. There are ***no*** SNQs that are "word-for-word" copies of the IPR grounds, and indeed, the primary reference that forms the vast basis for the rejections is entirely different and thus do not, and could not, use the prior IPR petition denial as a "roadmap."

Fourth, each of the above patents and publications are prior art to the Asserted Patents, and as mentioned above, the grounds of rejection outlined in this Request raise substantial new questions of patentability, because the reference combinations used to establish these grounds provide teachings not previously considered by the Office. None of the reference combinations used to establish the

grounds for rejection in this Request, nor the grounds themselves, were advanced by the Examiner during prosecution of the applications that matured into the Asserted Patents.

Further, the references are also non-cumulative because, as discussed in more detail below, the prior art reference individually and/or in combination disclose each and every limitation of the challenged claims—including the challenged independent claims that were allowed over the considered prior art.

For these reasons, the present request should not be denied pursuant to the CRU's discretionary powers.

V. LEVEL OF SKILL IN THE ART

The '905 patent claims priority to two provisional applications filed on December 20, 2004, and February 14, 2005. A person of ordinary skill in the art ("POSITA") at that time would have had a bachelor's degree in computer science or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent). More education could compensate for less experience and vice versa. Ex. 1003 at ¶13. Each of the arguments below is made from the standpoint of a POSITA in the field of the '905 patent. Requestor's expert, Dr. Benjamin Goldberg, was at least a POSITA at the time of the alleged invention. *Id.*; Ex. 1004.

VI. CLAIM CONSTRUCTION

The USPTO construes claims in accordance with their "broadest reasonable interpretation" ("BRI") in light of the claim language and specification. *In re Reuter*, 670 F.2d 1015, 1019 (C.C.P.A. 1981); *In re Smith International, Inc.*, 871 F.3d 1375, 1381, 1382-83 (Fed. Cir. September 26, 2017). This is as true in reexamination proceedings as it is during original prosecution. *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004); *In re ICON Health & Fitness, Inc.*, 496 F.3d 1374, 1379 (Fed. Cir. 2007). The USPTO broadly interprets claims during examination of a patent application because the applicant may "amend his claims, the thought being to reduce the possibility that, after the patent is granted, the claims may be interpreted as giving broader coverage than is justified." *In re Prater*, 415 F.2d 1393, 1404-05 (C.C.P.A. 1969). According to the Federal Circuit, "[t]his approach serves the public interest by reducing the possibility that claims, finally allowed, will be given broader scope than is justified. Applicants' interests are not impaired since they are not foreclosed from obtaining appropriate coverage for their invention with express claim language." *In re Yamamoto*, 740 F.2d 1569, 1571-72 (Fed. Cir. 1984) (*citing In re Prater*, 415 F.2d at 1405 n.31). The same policy underpinning the use of the broadest-reasonable-interpretation standard in initial examination, justifies its application in reexamination. *Id.*

Since the filing of the IPR, the District Court has issued a claim construction order construing terms as follows:

Claims	**Term**	**Construction**
1-3, 8-11,13-14	"ID code"	A unique code identifying a device
1, 9, 13	"access message"	A signal or notification enabling or announcing access

Ex. 1010 at 3. In addition to these terms, the Court also construed a number of terms as having their "plain meaning." *Id.* Although the terms above have been construed according to the *Phillips* standard, Requestor has applied these constructions in the discussion below, as the Broadest Reasonable Interpretation encompasses the *Phillips* standard. Accordingly, if the prior art meets the limitations construed according to the *Phillips* standard, it meets the limitations construed according to BRI.

A. "third party trusted authority" (claim 1)

In the previous IPR, the PTAB construed the term "third party trusted authority" as "an entity or party separate from the principal parties to a transaction." Ex. 1009, IPR2021-01447, Paper 12 at 13. In considering the prior art in light of its construction of the term, the PTAB found that Petitioner did not "explain[] sufficiently why Lapsley's DPC is a third-party trusted authority, what entities the DPC is a third-party relative to, or what application is being permitted to access in

the asserted combination." *Id.* at 24.[1] The Patent Owner argued that the DPC in Lapsley (which Petitioner pointed to as the "third party trusted authority") actually acted as a "cloud based digital wallet," and further that the purchaser did not access the digital wallet using a "fob" or "phone," but rather a device in the store where they were purchasing something. Ex. 1009 at p. 23-24. Based on these arguments, the PTAB found that the "the DPC is the resource to be accessed" and that "it is a party to the transaction, rather than a third party." *Id.* The PTAB further observed that during prosecution, the applicant explained that a "user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation." *Id.* at 24.

Requestor has applied this construction, in light of the Board's observations and analysis, to the prior art below.

VII. PRIORITY DATE OF THE '905 PATENT

The '905 patent claims priority to two provisional applications: U.S. Patent Application No. 60/637,538, filed December 20, 2004, and U.S. Patent Application No. 60/652,765, filed on February 14, 2005. Although Requestor does not concede that all 18 claims are entitled to one or both of the priority dates of the provisional

[1] Lapsley was the prior art reference that was relied upon for the "third party trusted authority" limitation in the IPR.

applications, all prior art references relied on in this petition date back to before December 20, 2004, and therefore, no further determination needs to be made regarding the priority date.

VIII. OVERVIEW OF THE TECHNOLOGY

The '905 patent relates to integrated wireless devices in a generic "computerized authentication" system that is used to gain access to devices, applications, or accounts through a biometric validation procedure. Ex. 1001 at 1:21-24, 1:49-54. The integrated device validates a user's biometric scan against biometric data stored on the device. *Id.* at 1:62-2:5. After validation using the biometric scan, a code stored on the device is transmitted to indicate that the user's identity has been verified. *Id.* The device transmits the code to a third-party trusted authority that determines if the code is authentic by checking it against a list of legitimate integrated device codes. *Id.* at 6:37-42. If the code is authentic, the user is allowed access to the device, application, or account they seek access to. *Id.* at 2:37-42. The '905 patent purports to solve for users the problem of having to "memorize or otherwise keep track of the[ir] credentials." *Id.* at 1:33-35. The patent also purports to solve the problem of illegitimate users "us[ing] a stolen access object to enter a secured location because the user's identity is never checked." *Id.* at 1:46-48.

IX. OVERVIEW OF THE PRIOR ART

A. Ludtke (Ex. 1005)

U.S. Patent No. 7,188,110 ("Ludtke") was filed on December 11, 2000. It issued on March 6, 2007. It is therefore prior art under 35 U.S.C. § 102(e) (pre-AIA).

Titled "Secure and Convenient Method and Apparatus for Storing and Transmitting Telephony-Based Data," Ludtke discloses a method of identifying an authorized user with a biometric device and enabling the authorized user to access private information. Ex. 1005 at Abstract. Ludtke recognizes both the need to ensure the integrity of financial information and the privacy of the user. *Id.* at 1:11-21.

The system disclosed in Ludtke is strikingly like the system disclosed in the '905 patent. The Ludtke system allows transactions through an eCommerce system through a "transaction device" that has a unique identifier (ID). *Id.* at 3:34-35. The transaction device can be a privacy card or a digital wallet or both. *Id.* at 3:35-39. This transaction device is a wireless device that is carried and maintained by a user. *See, e.g., id.* at 5:40-44. The transaction device includes a highly secured memory that can provide a transaction processing clearing house (TPCH) the necessary information to authorize a transaction. *Id.* at 3:40-45. The Ludtke system is described in Figure 1:

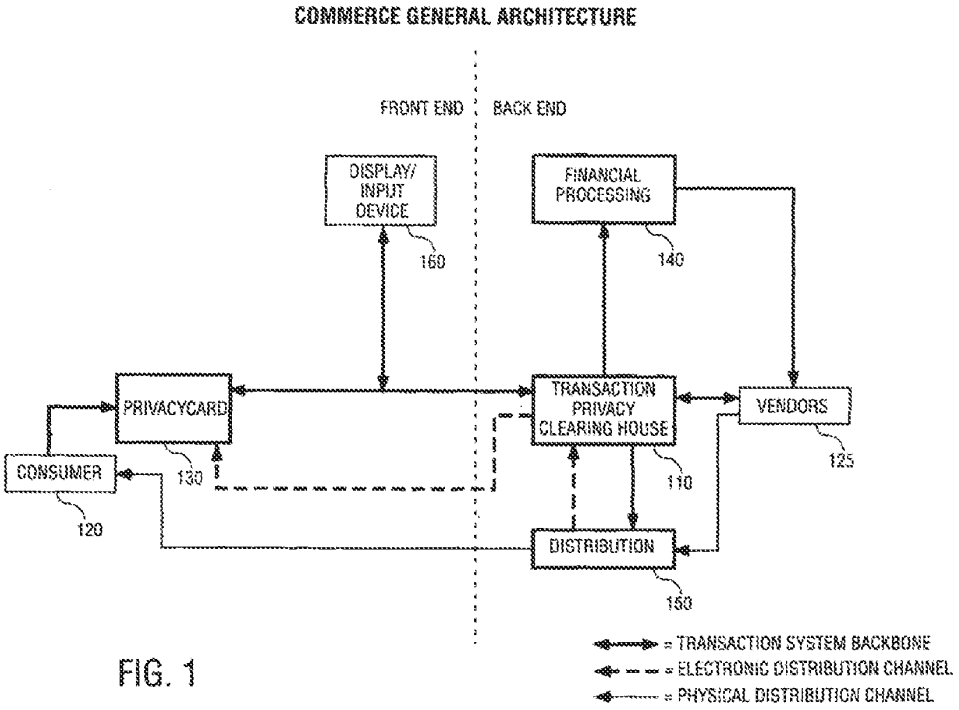


FIG. 1

As demonstrated in this figure, the Consumer 120 uses a transaction device 130 (in this figure, shown as a privacy card). The consumer wishes to purchase something from a vendor 125. The transaction device provides information to the TPCH for authorization for the transaction between the consumer and vendor to be performed. *Id.* at 6:36-44. The TPCH is not part of the transaction, but rather functions as a third-party middleman of the transaction. *Id.* at 7:44-46. This ensures that sensitive information is not shared with the vendor. *Id.* at 7:46-48.

Recognizing the need to protect the authorization of a user, Ludtke also discloses the use of fingerprint recognition as part of the digital wallet. *Id.* at 18:16-17. This biometric verification occurs before any transaction can take place, and therefore authorizes the user before the transaction device authorizes the device with the TPCH. *Id.* at 25:65-26:9; Ex. 1003 at ¶¶37-41.

B. Okereke (Ex. 1006)

U.S. Publication No. 2003/0196084 ("Okereke") was filed April 11, 2003. It published October 16, 2003. It is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA).

Okereke describes a "system and method for allowing users of wireless and mobile devices to participate in Public Key Infrastructure[PKI]" and also indicates that it "facilitates secure remote communications." Ex. 1006 at Abstract. Okereke states that "systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data." *Id.* at ¶3.

In setting up communications for a mobile device, Okereke specifically teaches that "a unique identifier for the wireless product to be employed is passed [sic] at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other

device capable of remote wireless communication. The unique identifier can be a serial number or SIM." *Id.* at ¶25.

Okereke describes the PKI: "With PKI, a public and private key are created simultaneously using the same algorithm by a certificate authority. Information encrypted by the private key can only be decrypted with the corresponding public key. The private key is given only to the requesting party, and the public key is made publicly available as part of a digital certificate in a directory that all parties can access. The private key is never shared with anyone or sent across the network." *Id.* at ¶ 7. Therefore, the private key is secret information. Ex. 1003 at ¶¶42-45.

C. Robinson (Ex. 1007)

U.S. Publication No. 2003/0177102 ("Robinson") was filed February 19, 2003. It published September 18, 2003. It is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA).

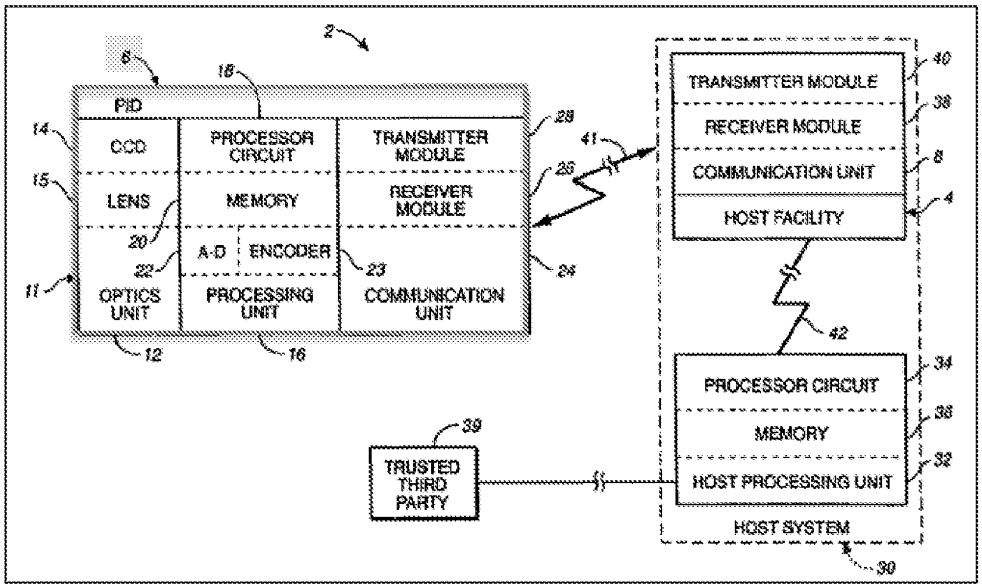
Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67, Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents

biometric and age-verifying information. *Id.* at ¶¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user; Ex. 1003 at ¶¶46-47.

D. Scott (Ex. 1008)

International PCT Application WO 99/56429 ("Scott") was filed on April 26, 1999. It was published on November 4, 1999. The International Publication Date is November 4, 1999, making it prior art under 35 U.S.C. § 102(b) (pre-AIA).

Scott discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1 [2]; Ex. 1003 at ¶48.

1. A POSITA Would Have Been Motivated to Combine the Teachings of the Ludtke, Okereke, and Robinson

Ludtke, Okereke, and Robinson all relate to protecting confidential information, communication over wireless networks, and the use of biometric information to protect this communication. All three references relate to communications for the purpose of financial transactions. Ex. 1005 at 4:54-56, 6:51-67; Ex. 1006 ¶3; Ex. 1007 ¶¶31-32, 47, Fig.1. A POSITA would naturally consider the teachings of Ludtke, Okereke, and Robinson in order to get a full understanding of the available options for secure communications and would have been motivated by this to combine the references' teachings. As explained in detail below, a POSITA would have considered applying the teachings of Okereke and Robinson to the teachings of Ludtke.

2. A POSITA Would Have Been Motivated to Combine the Teachings of Ludtke, Scott, and Robinson

Ludtke, Scott, and Robinson also relate to protecting confidential information over wireless networks, using biometric information to protect sensitive information, and also relates to financial information. Ex. 1005 at

[2] Annotations are added to figures unless indicated otherwise.

4:54-56, 6:51-67; Ex. 1007 ¶¶31-32, 47, Fig.1; Ex. 1008 at 10:24-32, 18:29-19:20. Therefore, a POSITA would have combined the Scott reference with Ludtke and Robinson for the same reasons above with respect to Okereke. In fact, a POSITA would have considered all of these references in trying to develop a process of secure communications.

X. DETAILED EXPLANATION OF THE PROPOSED REJECTIONS

As shown in detail below, claims 1-18 of the '905 patent are unpatentable under 35 U.S.C. § 103 in light of the prior art references and combinations of references presented below. The following rejections should be adopted in their entirety:

SNQ 1: Ludtke in combination with Okereke renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 2: Ludtke in combination with Okereke and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 3: Ludtke in combination with Scott renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (b) and (e) and 35 U.S.C. § 103; and

SNQ 4: Ludtke in combination with Scott and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102(a), (b), and (e) and 35 U.S.C. § 103.

A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1, 3-10, and 12-18 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 1 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1, 3-10, and 12-18 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

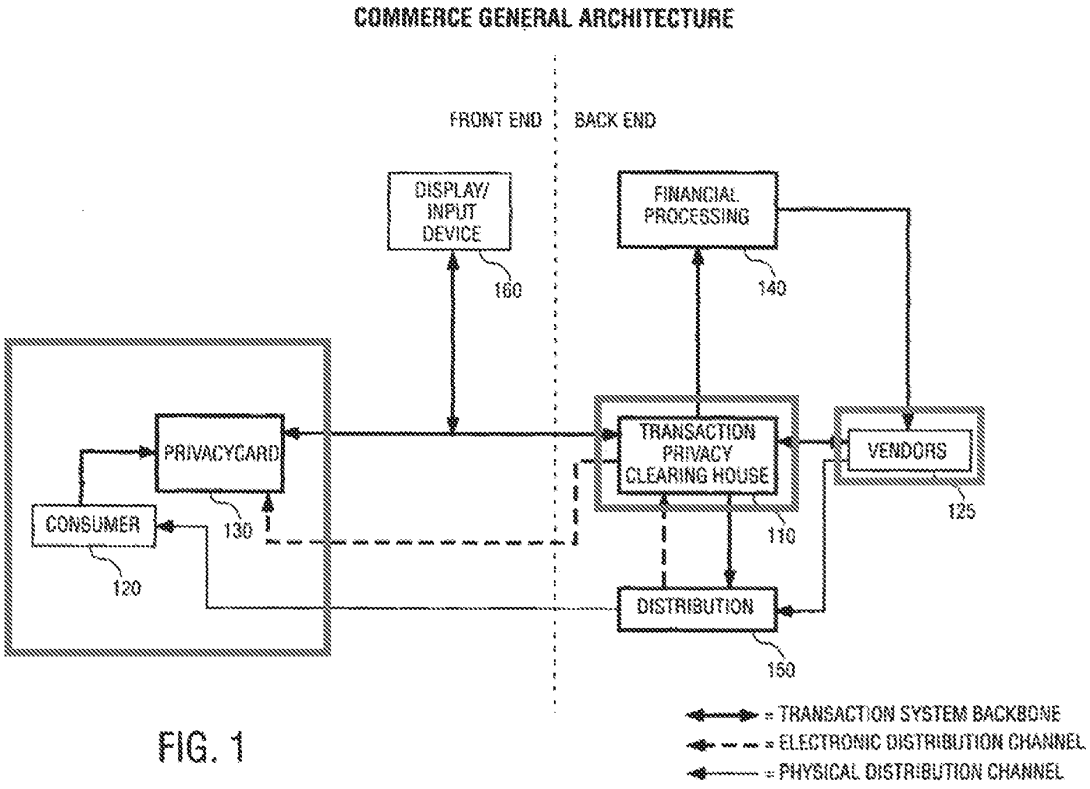


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third-party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Okereke discloses this "secret information."

Specifically, Okereke discloses a "secret key" that is maintained by the user, and can be used to encrypt and decrypt information communicated to the user. Ex. 1006 at ¶ 25.

The claims also require an "ID code" that identifies the user's device that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is unique. Okereke, however, does disclose this device ID code information, in the form of a unique serial number or SIM number for the user device. *Id*; Ex. 1003 at ¶¶196-198.

(b) A POSITA Would be Motivated to Combine Ludtke and Okereke

The scope and content of the prior art would have motivated a POSITA to combine Ludtke and Okereke. As explained above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID.

Ludtke discloses a persistent, tamper-proof memory, and a POSITA would have been motivated to combine the secret key disclosed in Okereke with the system disclosed in Ludtke. Ex. 1003 at ¶¶ 199-206. A POSITA would have

already known, as of the priority date of the '905 patent, that encryption using a secret key such as that as part of PKI would have been obvious when communicating confidential information. *Id.*

POSITAs specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. *Id.* The use of secret information to perform this type of encryption was well-known ***decades*** before the filing date of the '905 patent, and was a well-established, well-known method for implementing encryption. *Id.* Public Key Cryptography, which later developed into PKI encryption years before the '905 patent, was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* POSITA recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. *Id.* POSITA would therefore recognize that the use of PKI encryption, which is disclosed in Okereke, would make the system of Ludtke even more secure. *Id.* Okereke simply demonstrates this knowledge prior to the '905 patent's priority date.

Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a

financial transaction. A POSITA would have combined the teachings of Okereke's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. A POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or a SIM. Ex. 1003 at ¶¶199-206. Okereke explicitly discloses this fundamental information. Ex. 1006 at ¶25.

A POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor. *Id.* Indeed, both references are in the same field of endeavor as the '905 patent, *i.e.*, authentication of a user and device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:21-24 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed"); Ex. 1006 at Title ("System and method for secure wireless communication using PKI"); *id.* ¶31 ("In order to begin using the system via wireless device, the user may be required to provide

additional forms of authentication to the CPS, such as password or biometric signature.").

A POSITA would also have reasonably expected the combination of Ludtke and Okereke to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Given this disclosure in Ludtke, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Okereke as the transaction device information. A POSITA would have expected this to yield the predictable result of the option to use PKI-compliant encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number or SIM, and would have expected this combination to succeed. Ex. 1003 at ¶¶199-206.

For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the PKI-compliant encryption system because it had long been used as a way to encrypt and decrypt information and

share such information only for authorized users. Implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Okereke in the Ludtke system to further complement Ludtke's features. *Id.*

2. Claim 1

(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"

Ludtke and Okereke disclose this limitation.

An integrated device, biometric data, and an ID code: Ludtke discloses an integrated device, *e.g.*, Ludtke's "transaction device." Ex. 1005 at 3:32-35. Ludtke's transaction device provides a number of different "integrated" functions, including maintaining bills and bill paying on the device (*id.* at 4:4-6), online shopping (*id.* at 4:7-35), and downloading and accessing electronic catalogs (*id.* at 4:36-39). The transaction device includes a number of hardware options such as a magnetic stripe generator (*id.* at 3:49-51), a screen (*id.* at 55-57), and a bar code reader (*id.* at 3:61-63).

Ludtke explains that the "transaction device enhances security by ***authenticating the user of the card prior to usage***..." *Id.* at 4:62-65. This authentication can be performed by PIN code entry, or by other technologies such

as a biometric solution. *Id.* at 4:65-5:1. The biometric information ensures that the user is indeed legitimate.

Ludtke also specifically discloses authentication of a device through the use of "transaction device information." *Id.* at 6:36-44. A POSITA would recognize that this transaction device information necessarily includes unique device IDs, such as serial numbers and SIMs. Ex. 1003 at ¶¶208-212. But this knowledge of a POSITA is further embedded within Okereke. *See* Ex. 1005 at 6:36-44, *see also* Ex. 1006 at ¶30. As explained above in detail, a POSITA would have been motivated to combine the disclosure of Ludtke with the disclosure in Okereke.

Okereke also discloses a method for verifying a user during authentication of an integrated device. Okereke discloses wireless and mobile devices which are integrated devices. Ex. 1006 at Abstract. "The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication." *Id.* at ¶25.

Okereke specifically discloses authenticating the wireless device. Okereke describes a proxy server program awaiting initiation to establish secure wireless access capabilities. *Id.* at ¶25. When authentication is requested, "a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization." *Id.* "The unique identifier can be a serial number or

SIM number, for example." *Id.* Both serial numbers and SIM numbers are unique codes that identify the devices they are attached to. Ex. 1003 at ¶¶208-212. A POSITA would recognize that a serial number or SIM number is a unique identifier of a mobile device. *Id.* Once the proxy server confirms the unique identifier, it authorizes the device by sending approval to a desktop computer to make a key exchange to allow communication. *Id.*

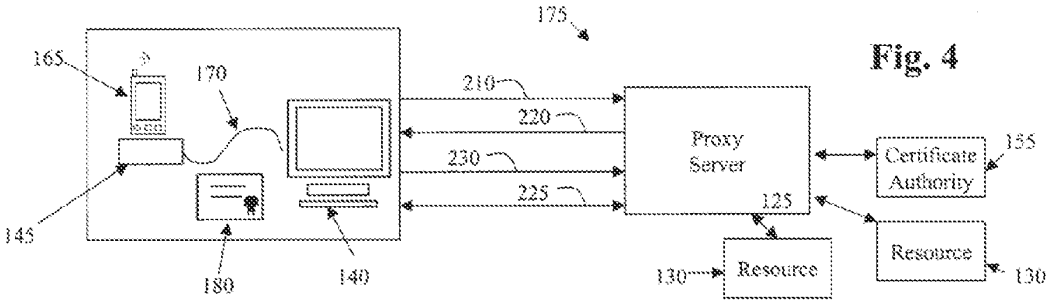


Fig. 4

Persistently storing biometric information and an ID code: Ludtke discloses a persistent storage on the integrated device. Specifically, the transaction device disclosed in Ludtke includes a process to use fingerprint data (biometric data of the user) to secure the device. Ludtke describes persistently storing the fingerprint data on the integrated device:

> The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If confirmation succeeds, the device writes the fingerprint image data into write once memory, or other memory that is protected from accidental modification.

Id. at 19:35-40. This fingerprint data is persistently stored in a tamper-proof format that is unable to be subsequently altered (write-once memory or other memory that is protected from accidental modification). Indeed, a write-once memory will only allow writing once, therefore, the information cannot be tampered with, and cannot be modified. Ex. 1003 at ¶213. In each case, this memory is persistent storage, because the information stored is not easily re-writable. *Id.*

(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;"

Ludtke describes receiving scan data from a biometric scan responsive to receiving a request for a biometric verification of the user. As explained above, Ludtke describes using biometric verification – including a fingerprint – to verify the user of the device. Figure 28 shows a device with a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input:

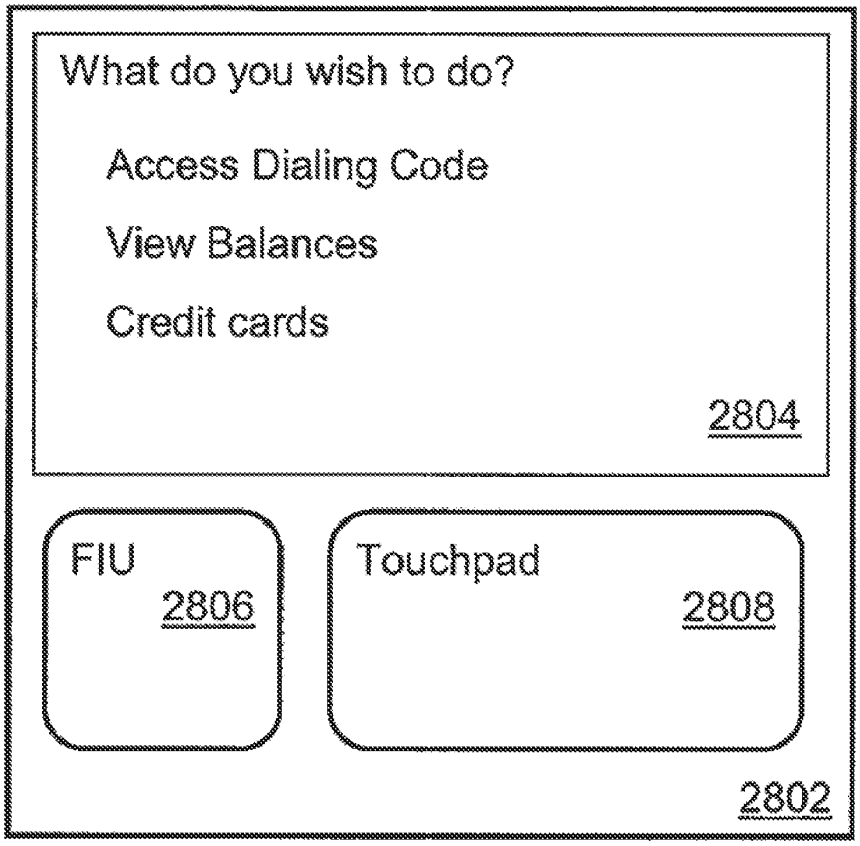


FIG. 28

Ex. 1005 at Fig. 28. "The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806." *Id.* at 39:24-27.

A POSITA would recognize that FIU 2806 is a "biometric sensor." Ex. 1003 at ¶215. Indeed, the only way the FIU would be able to detect the fingerprint – and

determine the data present in the fingerprint – is if it was a fingerprint (or biometric) sensor. *Id.*

Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

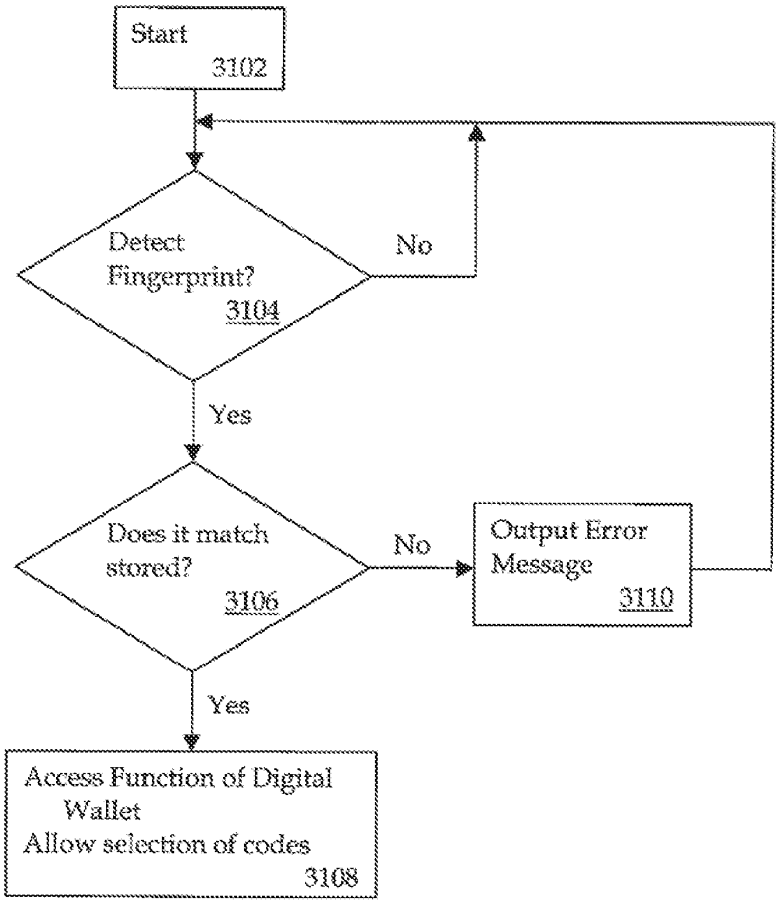


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, the device is continuously looking for a request for verification ("Detect fingerprint"). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106). *Id.* at 39:47-59.

(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"

Ludtke also shows this limitation in Figure 31:

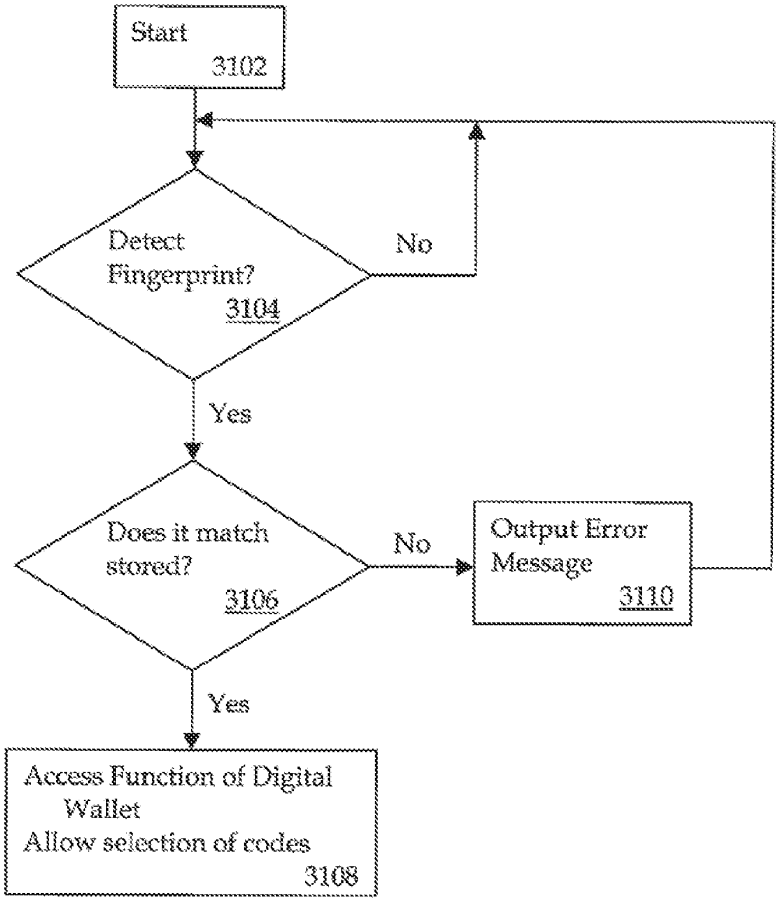


FIG. 31

Ex. 1005 at Fig. 31. Ludtke explains that if "a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW [Digital Wallet/Integrated Device] returns to checking to see if a fingerprint has been

detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes." *Id.* at 39:47-54.

(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

Responsive to a determination that the scan data matches the biometric data: As explained in conjunction with limitation [1c], if the scanned fingerprint data matches the stored fingerprint, then access to functions of the integrated device, such as the digital wallet, is permitted. *Id.* at 39:47-54.

Third party trusted authority: Ludtke describes a transaction processing [or privacy] clearing house (TCPH) which is a third party trusted authority. The TPCH "may access relevant account information to authorize transactions." *Id.* at 3:40-45. Figure 1 of Ludtke shows how the TPCH is a third party:

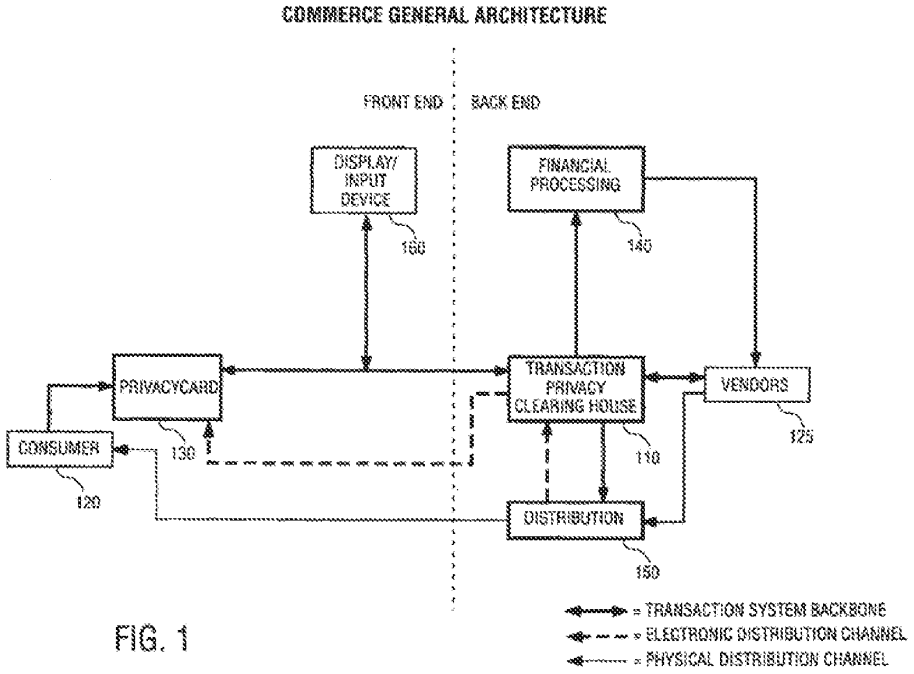


FIG. 1

Ex. 1005 at Figure 1. Figure 1 shows the commerce general architecture. *Id.* at 6:36-8:24. Figure 1 shows a consumer 120 who wishes to complete a purchase, *id.* at 6:36-64, and a vendor 125, who is selling something to the user 120. *Id.* "In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125." *Id.* at 6:36-38.

The TPCH is a third party to the transaction between the user/consumer 120 and the vendor 125. Ludtke explains that in "one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel.

This allows TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties." *Id.* at 7:44-48. This demonstrates that the TPCH acts as a middleman to ensure that only necessary information is exchanged between the consumer 120 and the vendor 125, but is not associated with either of them.

The TPCH is also a "trusted authority." Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. The consumer 120 and vendor 125 therefore trust the TPCH to indicate whether the transaction may be complete. Ex. 1003 at ¶¶ 219-221.

Wirelessly sending the ID code: Ludtke explains that "[t]he transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42; Ex. 1003 at ¶222.

One or more previously registered ID codes maintained by the third-party trusted authority: Ludtke also explains that the "TPCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction." *Id.* at 6:49-55. And as explained above, Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. Therefore, the TPCH includes previously registered information that can be compared with information from the consumer and the consumer's device so the TPCH can determine whether the consumer 120 is authorized to complete a transaction with vendor 125. Indeed, the transaction device information that the TPCH compares to the received transaction device information must be stored within the TPCH as a list of codes (and specifically, a list of ID codes), in order to perform the comparison function that is disclosed. *Id.* at 30:19-27; Ex. 1003 at ¶223.

ID Code: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure

database by the TPCH 110. *Id.* at 6:41-44. However, as discussed above, a POSITA would have been motivated to combine Ludtke with the teachings of Okereke, and would have recognized that the "transaction device information" would include a device serial number or SIM code, both of which uniquely identify the integrated device. Ex. 1003 at ¶224.

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction."

As indicated above, Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 ***and the user 120*** approval of the transaction to be performed." Ex. 1005 at 6:41-44. A POSITA would recognize that when the TPCH 110 "indicates to . . . the user 120," that indication is in the form of an access message allowing the user access to an application. Ex. 1003 at ¶225. In this case, the TPCH is allowing access to the application on the transaction device that will permit the transaction to be completed. Specifically, the TPCH is sending a signal (or a notification) to the user's device, which allows (it enables or announces) access to the application on the transaction device that will permit the transaction to be completed. Ludtke further discloses this limitation at Fig. 15, Step 1520:

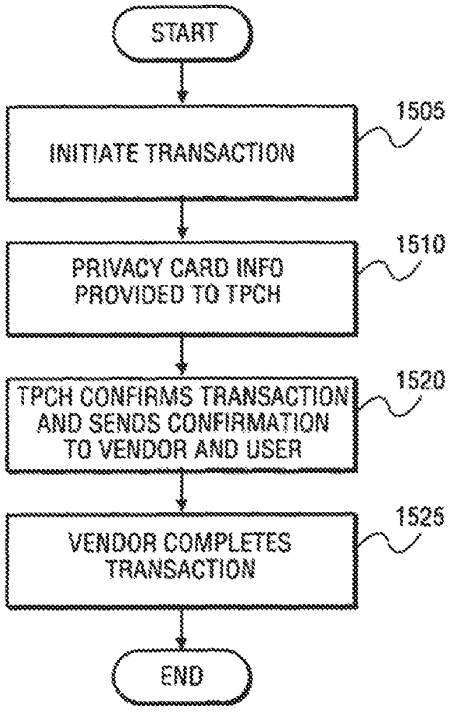


FIG. 15

Ex. 1005 at Fig. 15, *see also* Fig. 17, steps 8 and 9-1. With regard to step 1520, Ludtke teaches that the "TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525, the vendor completes the transaction without the knowledge of the user." *Id.* at 27:13-16. The transaction, as described in Ludtke, is a financial transaction because it is a purchase from a vendor by the user. Ex. 1003 at ¶225.

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."

Ludtke and Okereke disclose this limitation. As explained above, Ludtke discloses the transaction device receiving biometric information allowing access to the device and then subsequently communicates the ID code to the TPCH. Ex. at 1003 at ¶226. It is inherent that, when the ID code is sent to the TPCH, that is an indication that the biometric verification has been successful. Indeed, as the ID code will not be sent at all if biometric verification fails (Ex. 1005 at 19:35-45), the sending of the ID code itself is an "indication that the biometric verification was successful." *Id.*

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."

Ludtke describes a number of different types of biometric information that may be used: "The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, ***fingerprint***, ***retinal scan***, ***voice***, DNA, ***hand profile***, ***face recognition***, etc." Ex. 1005 at 35:60-64; Ex. 1003 at ¶227.

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet,

laptop, mp3 player, mobile gaming device, watch and a key fob."

Ludtke and Okereke disclose this limitation. POSITA would recognize that the transaction device disclosed in Ludtke, which includes a number of different iterations, including a privacy card (Ex. 1005 at 20:43-50), and a cellular telephone mechanism (*id.* at 17:3-10), would meet many of these limitations including "mobile phone," "tablet," and "key fob." Okereke explicitly states that its device may be a mobile phone. Ex. 1006 at Abstract; Ex. 1003 at ¶228.

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application."

Ludtke discloses this limitation. In Ludtke, access would be given applications of either computer software, a file (or both). In a number of embodiments, Ludtke describes the transaction device as including a "digital wallet" which POSITA would recognize as an application and files that allow a user to digitally store credit card and other payment information and to make transactions with that card. Ex. 1005 at 5:1-5; Ex. 1003 at ¶229.

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."

Ludtke discloses this limitation. In Ludtke, access would be given applications of either computer software, a file (or both). In a number of

embodiments, Ludtke describes the transaction device as including a "digital wallet" which POSITA would recognize as files that allow a user to digitally store credit card and other payment information and to make transactions with that card. Ex. 1005 at 5:1-5; Ex. 1003 at ¶230. Moreover, a POSITA would recognize that giving access to the digital wallet is providing access to a financial account. *Id.*; Ex. 1003 at ¶230.

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data."

Ludtke and Okereke disclose this limitation. For example, Ludtke discusses the process of requesting and receiving biometric information. *See supra* Section X.A.2; Ex. 1005 at 39:19-35. Ludtke then describes an embodiment where the biometric information is not needed: "Alternatively, the consumer access device, once the user has been identified may not require re-identification until the consumer access device is, for example, turned off." *Id.* at 39:35-38. A POSITA would recognize that in this embodiment, a request to authenticate the device for a financial transaction after biometric verification had occurred, but before the device was turned off is a request to send the ID code without an additional biometric

verification. Ex. 1003 at ¶231. A POSITA would recognize that in this case, the ID code would be sent without biometric verification. *Id.*

9. Claim 9:

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;"

See Claim 1, element [1a]. Section X.A.2.a, *supra*; Ex. 1003 at ¶232.

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and"

See Claim 1, elements [1c], [1d]. Section X.A.2.c, d, *supra*.

The "validation module" will be the portion of the smartphone, including processors and instructions that receives the scan and verifies the biometric information. Ex. 1003 at ¶234. A POSITA would recognize that the validation module would be in coupled with the memory, since the biometric information that the validation module compares with received biometric information is stored in the memory for comparison. *Id.*

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third -party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based

on the comparison of the ID code and allowing the user to—complete a financial transaction."

See Claim 1, elements [1d], [1e]. Section X.A.2.d, e, *supra*. A POSITA would recognize that because the transaction device has wireless access, it necessarily has a "radio frequency communication module," as all wireless communications occur through an RF module. Ex. 1003 at ¶235.

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."

Ludtke and Okereke disclose this limitation. As explained above, Ludtke explains that "[t]he transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42. Therefore, the communications described above in conjunction with claim 1 (by both Ludtke and Okereke) to the agent are transmitted over a network. Ex. 1003 at ¶236.

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone,

tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."

See Claim 5. Section X.A.5, *supra*; Ex. 1003 at ¶237.

12. Claim 13:

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and"

See Claim 1, elements [1a], [1d], [1e]. Section X.A.2.a, d-e, *supra*. The integrated devices described above are hardware devices because they are held by the user. Ex. 1003 at ¶238. The "authentication circuit" is the portion of the hardware device, including processors and instructions that receives the scan and verifies the biometric information. *Id.*

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a

comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

See Claim 1, elements [1d], [1e]. Section X.A.2.d-e, *supra*; Ex. 1003 at ¶239.

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."

See Claim 1, elements [1b], [1c]. Section X.A.2.b-c, *supra*. Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

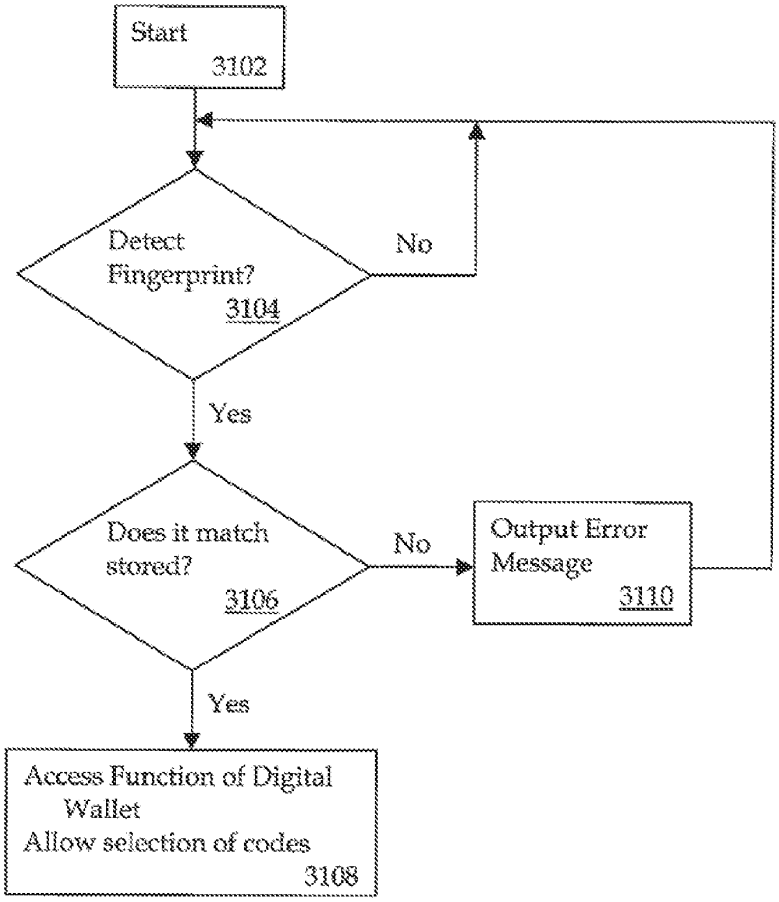


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, if the scan data does not match the stored data (i.e., the device cannot authenticate the user), it will output an error message, and not allow access to the digital wallet or selection of codes. *Id.* at 39:47-59. Ex. 1003 at ¶¶240-241.

14. **Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."**

See claim 5, section X.A.5, *supra*; Ex. 1003 at ¶242.

15. **Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition."**

See claim 4, Section X.A.4, *supra*; Ex. 1003 at ¶243.

16. **Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account."**

See claim 7, Section X.A.7, *supra*; Ex. 1003 at ¶244.

17. **Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application."**

See claim 6, Section X.A.6, *supra*; Ex. 1003 at ¶245.

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 2 and 11 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 2 relies entirely on Ludtke and Okereke for the same reasons as outlined in SNQ 1, but also relies on Robinson for the limitations in dependent claims 2 and 11. Both of these dependent claims involve registering an age

verification. Where Ludtke and Okereke do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 2 and 11. As explained below, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Okereke. Ex. 1003 at ¶246.

(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Okereke

The scope and content of the prior art would have motivated POSITA to combine Robinson with Ludtke and Okereke. Ex. 1003 at ¶¶247-250. Like both Ludtke and Okereke, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67, Fig. 1.

All three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. *Id.* at ¶9-10; Ex. 1003 at ¶¶247-250. A POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, a POSITA would have recognized that the age verification disclosed in Robinson would, for example, allow a way for the Ludtke system to ensure that the user is

old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area. *Id.*

A POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. *Id.* Robinson, like Ludtke and Okereke, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Okereke to also include the age of the user who was verified with biometric information. *Id.* The age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals. *Id.*

2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the ID code."

Ludtke in combination with Okereke disclose all of the limitations of claim 1. *See* SNQ 1, Claim 1. Section X.A.2, *supra.*

However, neither Ludtke nor Okereke expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67, Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a

user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents biometric and age-verifying information. *Id.* at ¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user. Ex. 1003 at ¶252.

3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the ID code.

Ludtke in combination with Okereke disclose all of the limitations of claim 9. *See* SNQ 1, Claim 9. Section X.A.9, *supra*; Ex. 1003 at ¶253.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 11 for the same reasons as described in conjunction with claim 2. Section X.B.2, *supra*. Ex. 1003 at ¶254.

C. SNQ 3: Ludtke in combination with Scott Renders Claims 1, 3-10, and 12-18 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 3 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1, 3-10, and 12-18 except the "unique Device ID" and storage

of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

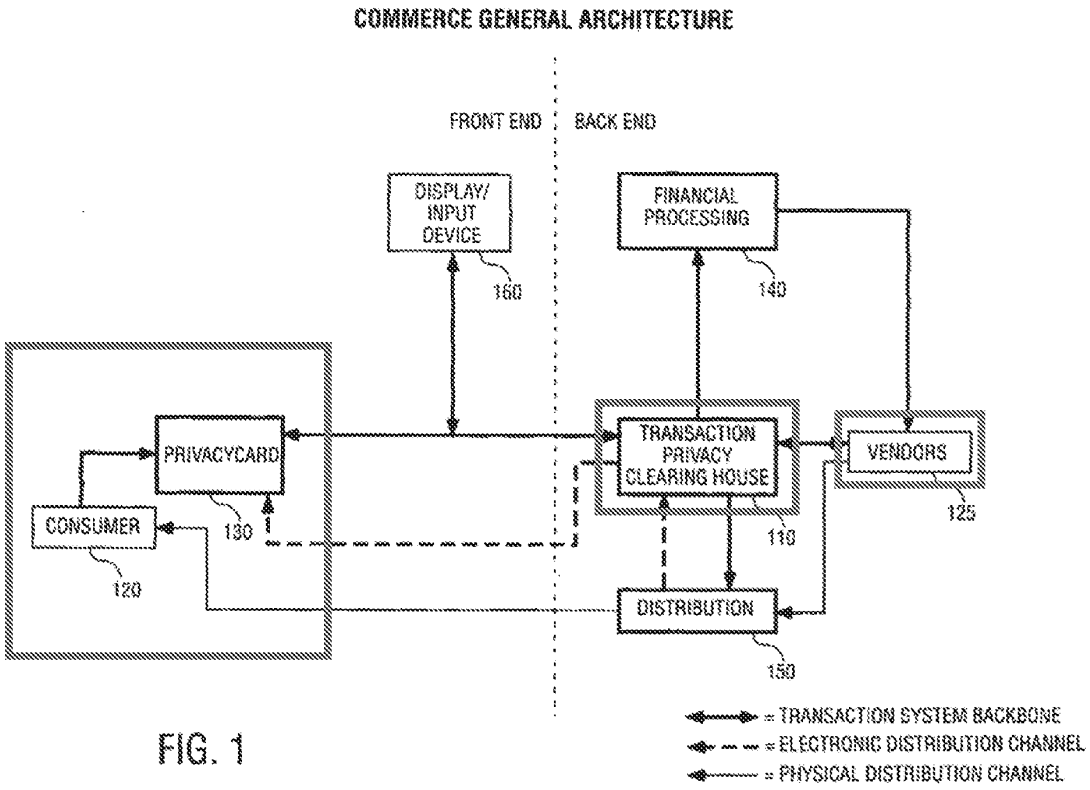


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information.

Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Scott discloses this "secret information." Specifically, Scott includes an extensive discussion regarding a secret key infrastructure. Scott discloses that the device's memory 20 also stores a private key unique to each device and used for encryption, which can be "set into memory by the manufacturer." Ex. 1008 at 11:24-30, 28:13-15, 4:14-18. Scott discloses that this "private key" used by the PID 6 is never disclosed. *Id.* at 8:21-22.

The claims also require a unique "ID code" that identifies the user's device that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is unique. Scott, however, does disclose a unique ID code that identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including a unique ID code that identifies the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. Serial numbers are unique codes that identify the devices that they are attached to. Ex. 1003 at ¶¶255-258. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

(b) A POSITA Would be Motivated to Combine Ludtke and Scott

The scope and content of the prior art would have motivated POSITA to combine Ludtke and Okereke. As explained above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique"

nature of a device ID code. Similar to Ludtke, Scott discloses authenticating a user using a "personal identification device" (PID) for protected applications such as opening a hotel room door or a conducting a point-of-sale transaction. *Id.* at 8:5-12. Scott specifically describes a system for authentication of a mobile device to protect information for financial transactions. *Id.* at 2:5-16.

Ludtke discloses a persistent, tamper proof memory, and POSITA would have been motivated to combine the secret key disclosed in Scott with the system disclosed in Ludtke. Ex. 1003 at ¶¶259-265. The secret key infrastructure disclosed in Scott is similar to that disclosed in Okereke, as discussed above. *Id.* As discussed above, a POSITA would have already known, as of the priority date of the '905 patent, that encryption using a secret key such as that disclosed in Scott would have been obvious when communicating confidential information. *Id.* A POSITA specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. *Id.* The use of secret information (such as that in PKI encryption) to perform this type of encryption was well-known ***decades*** before the filing date of the '905 patent, and was a well-established, well-known method for implementing encryption. *Id.* For example, Public Key Cryptography, which later developed into PKI encryption years before the Challenged Patents,

was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* A POSITA recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. *Id.* A POSITA would therefore recognize that the use of secret information, which is disclosed in Scott, would make the system of Ludtke even more secure. *Id.* Scott simply demonstrates this knowledge prior to the '905 patent's priority date.

Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. A POSITA would have combined the teachings of Scott's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. A POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or other number that is specific to the processing unit. Ex. 1003 at ¶¶259-265. Scott explicitly discloses this fundamental information. *Id.*

A POSITA would have been motivated to combine Ludtke and Scott because they are both in the same field of endeavor. Indeed, both references are in the same field of endeavor as the '905 patent, *i.e.*, authentication of a device,

including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:21-24 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ludtke at Abstract ("A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed"); Scott at Abstract ("A portable, hand-held personal identification device (6) and method for providing secure access to a host facility…"); *id.* ¶31 ("Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility").

A POSITA would have reasonably expected the combination of Ludtke and Scott to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Scott similarly discloses a persistent, tamper-proof memory. Scott teaches that data is stored in a memory where, after biometric enrollment, "there is no going back or editing." Ex. 1008 at 16:11-12. Given these disclosures, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret

information in Ludtke's memory and using the unique device ID disclosed in Scott as the transaction device information. A POSITA would have expected this to yield the predictable result of the option to use secret key encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number, and would have expected this combination to succeed. Ex. 1003 at ¶264.

For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the secret key encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. Implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Scott in the Ludtke system to further complement Ludtke's features. Ex. 1003 at ¶265.

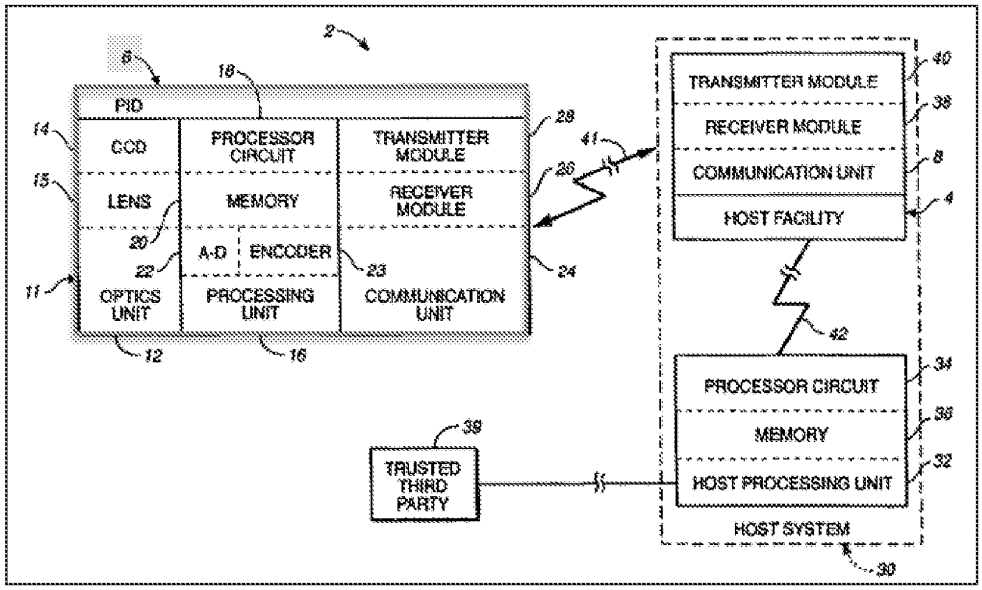
2. Claim 1

(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.a, *supra*.

As explained above in detail, a POSITA would have been motivated to combine the disclosure of Ludtke with the disclosure in Scott.

Scott also discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1.

As explained above, Scott discloses that the memory 20 of the PID 6 persistently stores a plurality of codes and other data values including a unique ID code that identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including a unique ID code that identifies the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. A serial number is a unique code that identifies the device it is attached to. Ex. 1003 at ¶¶267-270. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

As discussed above, a POSITA would have been motivated to modify the system of Ludtke to incorporate the unique serial numbers also disclosed in Scott. Ex. 1003 ¶¶267-270; *see supra* §X.C.1. A POSITA would have been motivated to store permanent information, such as the unique device identifiers (serial number). Moreover, a POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Scott, which would ensure that the information used to authenticate the device only identifies the authorized device. *Id.* A POSITA would also have stored the unique device identifiers in the persistent tamper-proof memory, because this is important information that allows authorization and sensitive communications to take place, and a POSITA would have recognized the need to take care to ensure it is not easy to tamper with and modify the information. *Id.* at ¶270.

(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.b, *supra*. Ex. 1003 at ¶271.

(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.c, *supra*. Ex. 1003 at ¶272.

(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.d, *supra*; Ex. 1003 at ¶273.

ID Code: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure database by the TPCH 110. Ex. 1005 at 6:36-64. However, as discussed above, a POSITA would have been motivated to combine Ludtke with the teachings of Scott, and would have recognized that the "transaction device information" would include a unique serial number, which uniquely identifies the integrated device. Ex. 1008 at 4:1-14, 5:10-21; Ex. 1003 at ¶274.

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully

authenticated the ID code, allowing the user to complete a financial transaction."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.e, *supra*; Ex. 1003 at ¶275.

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.3, *supra*. Ex. 1003 at ¶276.

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.4, *supra*. Ex. 1003 at ¶277.

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.5, *supra*. Ex. 1003 at ¶278.

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.6, *supra*. Ex. 1003 at ¶279.

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.7, *supra*. Ex. 1003 at ¶280.

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.8, *supra*. Ex. 1003 at ¶281.

9. Claim 9:

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.9.a, *supra*. Ex. 1003 at ¶282.

See also Claim 1, element [1a]. Section X.C.1.a, *supra*.

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against

one or more previously registered ID codes maintained by the third-party trusted authority; and"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.9.b, *supra*. Ex. 1003 at ¶284.

See also Claim 1, elements [1c], [1d]. Section X.C.1.c, d, *supra*. Ex. 1003 at ¶285.

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third -party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.9.c, *supra*. Ex. 1003 at ¶286.

See also Claim 1, elements [1d], [1e]. Section X.A.1.d, e, *supra*. Ex. 1003 at ¶287.

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.10, *supra*. Ex. 1003 at ¶288.

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone,

tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.11, *supra*. Ex. 1003 at ¶289.

See also Claim 5. Section X.C.5, *supra*. Ex. 1003 at ¶290.

12. Claim 13:

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.12.a, *supra*. Ex. 1003 at ¶291.

See also Claim 1, elements [1a], [1d], [1e]. Section X.A.1.a, d-e, *supra*. Ex. 1003 at ¶292.

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a

comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.12.b, *supra*. Ex. 1003 at ¶293.

See also Claim 1, elements [1d], [1e]. Section X.A.1.d-e, *supra*. Ex. 1003 at ¶294.

13. **Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."**

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.13, *supra*. Ex. 1003 at ¶295.

See Claim 1, elements [1b], [1c]. Section X.A.1.b-c, *supra*. Ex. 1003 at ¶296.

14. **Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."**

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.14, *supra*. Ex. 1003 at ¶297.

See also claim 5, section X.C.5, *supra*. Ex. 1003 at ¶298.

15. **Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a**

facial recognition, a signature recognition, and a voice recognition."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.15, *supra*. Ex. 1003 at ¶299.

See also claim 4, Section X.C.4, *supra*. Ex. 1003 at ¶300.

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.16, *supra*. Ex. 1003 at ¶301.

See also claim 7, Section X.C.7, *supra*. Ex. 1003 at ¶302.

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.17, *supra*. Ex. 1003 at ¶303.

See also claim 6, Section X.A.6, *supra*. Ex. 1003 at ¶304.

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 2 and 11 Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 4 relies entirely on Ludtke and Scott for the same reasons as outlined in SNQ 3, but also relies on Robinson for the limitations in dependent claims 2 and

11. Both of these dependent claims involve registering an age verification. Where Ludtke and Scott do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 2 and 11. As explained below, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Scott. Ex. 1003 at ¶¶305-307.

(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Scott

The scope and content of the prior art would have motivated a POSITA to combine Robinson with Ludtke and Scott. Ex. 1003 at ¶¶308-311. Like both Ludtke and Scott, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67, Fig. 1.

All three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. Ex. 1007 at ¶9-10; Ex. 1003 at ¶¶308-311. A POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, a POSITA would have recognized that the age verification disclosed in

Robinson would, for example, allow a way for the Ludtke system to ensure that the user is old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area. Ex. 1003 at ¶310.

A POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. Ex. 1003 at ¶311. Robinson, like Ludtke and Scott, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Scott to also include the age of the user who was verified with biometric information. Ex. 1003 at ¶¶308-311. The age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals. *Id.*

2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.

Ludtke in combination with Scott disclose all of the limitations of claim 1. *See* SNQ 3, Claim 1. Section X.C.2, *supra*. Ex. 1003 at ¶312.

However, neither Ludtke nor Scott expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson discloses this limitation as described in SNQ 2. *See* Section X.B.2; *see also* Ex. 1003 at ¶313.

3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the device ID code.

Ludtke in combination with Scott disclose all of the limitations of claim 9. *See* SNQ 3, Claim 9. Section X.C.9, *supra*. Ex. 1003 at ¶314.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 11 for the same reasons as described in conjunction with claim 2. Section X.D.2, *supra*. Ex. 1003 at ¶315.

XI. REAL PARTIES OF INTEREST

Requestor certifies that Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. are the real parties-in-interest.

XII. CONCLUSION

For at least the reasons cited herein, the prior art references cited in this Request present substantial new questions of patentability with respect to the Challenged Claims of the '905 patent. Accordingly, the Office should declare a reexamination of these claims and reject them on at least the SNQs detailed in this Request.

DATED: June 8, 2022

Respectfully submitted,

By */s/ Marissa Ducca*

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005
Email: marissaducca@quinnemanuel.com
Phone: (202) 538-8000
Fax: (202) 538-8100

James M. Glass (Reg. No. 46,729)
Quinn Emanuel Urquhart & Sullivan, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email : jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

Attorneys for Third-Party Requestor Samsung Electronics America, Inc.