Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems

A Smart Card Alliance White Paper

May 2002

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

Executive Summary

Why Are Secure Identification Systems Needed?

Both government and commercial organizations are implementing secure personal identification (ID) systems to improve confidence in verifying the identity of individuals seeking access to physical or virtual locations. A secure personal ID system is designed to solve the fundamental problem of verifying individuals are who they claim to be. This verification is achieved using a recognized ID credential issued from a secure and effective identity confirmation process. A secure personal ID system design will include a complex set of decisions to select and put in place the appropriate policies and procedures, architecture, technology and staff to deliver the desired level of security. A secure ID system can provide individuals with trusted credentials for a wide range of applications — from enabling access to facilities or secure networks, to proving an individual's rights to services, to conducting online transactions.

Biometric and Smart Card Technologies Provide Highest Security

Biometric technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics. Biometric technologies, when used with a well-designed ID system, can provide the means to ensure that an individual presenting a secure ID credential has the absolute right to use that credential. Smart cards have the unique ability to store large amounts of biometric and other data, carry out their own on-card functions, and interact intelligently with a smart card reader. Secure ID systems that require the highest degree of security and privacy are increasingly implementing both smart card and biometric technology.

Combining Biometrics and Smart Cards Delivers Economic and Security Advantages

In an ID system that combines smart card and biometric technologies to verify the identity of individuals, a "live" biometric image (e.g., scan of a fingerprint or hand geometry) is captured at the point of interaction and compared to a stored biometric image that was captured when the individual enrolled in the ID system. Smart cards provide the secure, convenient and cost-effective ID technology that stores the enrolled biometric template and compares it to the "live" biometric template. A secure ID system using smart card and biometric technology provides:

- Enhanced privacy, securing information on the card, allowing the individual to control access to that information and removing the need for central database access during identity verification.
- Improved security, protecting information and processes within the ID system and actively authenticating the trust level of the environment before releasing information.
- Improved ID system performance and availability through local information processing and contactless ID card and reader implementations.
- Improved system return on investment through the flexibility and upgradability that smart cards provide, allowing support of different authentication methods and multiple, evolving applications.

About this White Paper

This white paper was developed by the Smart Card Alliance Secure Personal Identification Task Force to discuss the combination of smart card and biometric technology in secure ID systems. The paper provides a basic tutorial of the components that are included in a secure identification system that uses biometric and smart card technology. It defines the terminology used to describe a biometric ID system and discusses the key questions that should be considered when designing the architecture of a secure ID system that incorporates both smart cards and biometrics. The paper concludes with a discussion of how the combination of smart card and biometric technology enhances the security, privacy, performance and cost-effectiveness of a secure ID system, while enhancing trust and convenience for individuals.

The paper provides answers to questions commonly asked about secure ID system implementations, including:

- What is a secure ID system?
- What are biometrics and how do they work?
- What makes an ID system secure?
- What are the policy considerations for a secure ID system?
- How can individual privacy be protected in a secure ID system?
- How can the combination of biometric and smart card technologies provide the highest security, while also protecting privacy?

What Is a Secure Identification System?

In today's culture nearly every person carries multiple types of identification cards (or credentials) issued by many different public and private organizations. These credentials range from driver's licenses through membership cards, credit cards and corporate identification. The primary purpose of these credentials is to identify the cardholder as having the rights, privileges, and responsibilities indicated by the issuer of that credential.

As the privileges associated with these cards gain more value, assuring the authenticity of the ID card and the identity of the cardholder becomes more important. If, for example, the credential is used to access corporate databases, enter into restricted areas, drive a car, or enter a country, it becomes essential that the identification process use appropriate security measures and technologies to deter both impersonation and counterfeiting and to assure the privacy of information on the card. To implement the desired security level for an application, a secure ID system must ensure that:

- Policies and procedures are in place for both issuing and monitoring the use of the credential;
- System life cycle management procedures have been established;
- Training for users and issuers has been implemented;
- A system has been established to protect access to the ID holder's information and to prevent unauthorized viewing or tampering;
- A security control is in place to provide access to information on the ID credential to authorized viewers;
- The ID credentials are issued only by the authorized issuing organization;
- The identity of the individual applying for the credential has been established;
- The person to be granted access to the privileges indicated by the credential is indeed entitled to them; and
- The credential is issued to the correct person.

A secure ID credential is the interface between an individual seeking some form of access and the system or facility to which access is desired. The ID card will contain or reference information that is used to verify the individual's identity and permissions. To be a trusted secure personal credential, the reader of the credential must be able to establish that a legitimate authority issued the credential and that the data it contains was created by the legitimate authority, has not been altered, and is associated with that specific credential.

The decision to create a secure ID system that includes both smart card and biometric technology typically results from a security threat analysis that determines a need for a system that can ensure the highest degree of security.

Components of a Secure Identification System

To implement an efficient and effective secure ID system, many factors need to be considered. A secure ID system implementation can include a visual inspection, use of a personal identification number (PIN), use of a machine-readable card incorporating a magnetic stripe, bar code, integrated chip or optical memory, or use of a biometric measurement. Applications may also use a combination of these technologies to meet specific security and system requirements.

Once the purpose of the secure ID system has been determined, the appropriate components for its implementation, security architecture and distribution life cycle process must be assembled.   Figure 1 lists a general set of components required by most secure ID systems and examples of the decisions that need to be made for each component.

Figure 1 - Secure ID System Components

Secure ID System Component	Key Design Decisions
ID Credential / Card	• Types of applications supported now and in the future • Design (what it will look like, what information is on the card, whether anti-counterfeiting and anti-tampering features are needed, whether a photo is needed) • Usage (how often the card is used and under what conditions) • Required memory capacity • Appropriate operating system • Type of card technology • Security certification level
Network & Infrastructure	• Distributed or centralized communications • Implementation of trusted channels • Design of secured environments • Support for local, regional or central issuance • Distribution of trusted materials • Reader infrastructure design • Control and management of system access
Trusted Issuing Authority	• Use of x.509 certificates or other digital certification mechanisms • Use of a commercial trusted authority for the creation, protection, and distribution of certificates or in-house creation of certificates in a protected environment • Types of algorithm(s) to be implemented • Key management processes
Cryptography	• Selection of encryption technology • Implementation of symmetric or asymmetric keys • Number of keys issued and desired size of key space
Biometrics	• Biometrics used (e.g., fingerprint, facial, iris scan) • Algorithm used to process the biometric information • Number and location of stored biometric measurements • Conditions under which biometrics will be used • Storage of full or compressed biometric images
Enrollment Stations	• Environment and location of enrollment stations • Method for operator self-authentication • Method for verifying the credential applicant's identity • Interaction of stations with the network
Issuance Process	• ID card personalization process • Compliance of the distribution process with the defined security policy • Implementation of card inventory physical security • Management of the audit of cards • Implementation of data security • Life cycle management process
Readers	• Location, number, architecture, and protection of card readers • Design and appearance of the readers • Authentication of readers by the ID card • Management of security features and security certification level • Secure communication with the network • Manufacturing processes for readers

Key Attributes of a Secure ID System

In an increasing number of implementations, the same ID card is being used for multiple applications, further increasing the need for highly secure technologies and effective and efficient ID verification processes. This section describes key attributes of the secure ID credential, the system security policies and procedures, and the secure ID system staffing and training.

Secure Personal ID Credential

- ***Physical Security***. ID cards are often examined by individuals who have minimal special equipment to validate card authenticity or minimal motivation to inspect the card in detail. The card, therefore, must have sufficient observable physical security features to allow a quick visual verification and offer significant deterrents for a counterfeiter or forger. Well-designed visual security features can establish a reasonable level of trust and can include security printing, covert inks, optical variable inks, and optical variable devices.

- ***Data Security***. Privacy, authenticity, and integrity of data encoded on the credential are primary requirements for a secure ID system. Sensitive data is typically encrypted, both on the ID card and during communications with the reader system. Digital signatures may be used to ensure data integrity, with multiple signatures required if different authorities created the data. To ensure privacy, applications and data on the ID credential are designed to prevent information sharing.

- ***Identity Verification***. The ID card can contain trusted biometric or other data that will assist with the confirmation of the user’s identity. In many situations, especially at unstaffed locations, an ID card and reader perform the entire identity verification.

- ***Challenges and Privacy***. For the highest security and privacy, the secure ID system may require that system components authenticate the legitimacy of other components during the identity verification process. This can include the ID credential verifying that the automated reader is authentic and that the requesting system has the right to access the information being requested.

System Security Policies and Procedures

Security policies and procedures are administrative documents created by the issuing organization to specifically articulate the entire security structure and its integration into the organization. A strong and well-designed set of security policies and procedures provides confidence, reliability, and clear directions for all personnel involved with the secure ID system.

People

The integrity and trust of the people operating, managing and using the secure ID system are very important and their performance is essential to overall system security and reliability. This includes the system administrators, issuing agents, and security officers, guards and personnel that staff the points of interaction where the ID cards are being used.

Training
Training in the issuance, examination, and use of credentials is crucial to a successful secure ID system. Creators of credentials must be fully aware of and support the security policies and procedures on how to create, protect associated sensitive information, distribute, and audit credentials. Inspectors are directly responsible for accurately examining credentials and being aware of fraud attempts (such as forgery, counterfeiting or attempts by an impostor or impersonator). Credential users must understand the care, usage, and control of the ID card and be provided with clear instructions on how the credential interfaces with reading systems.

Secure Identification Systems and Privacy

Protection of an individual's privacy has long been a concern when considering a centralized ID system and has received increased attention in recent discussions about ID card programs in the US.[1] The issue is often viewed as a conflict between the need for security and the rights of privacy.

When an individual enrolls in an ID system, a relationship is formed between the individual and the organization issuing the ID. In this relationship, the individual confirms that the organization has the need to know and use their personal information for identification, and possibly other, purposes. Conversely, the organization issuing the ID, in accepting the enrollment, assumes a duty to protect the member's information and use it appropriately. As a result, a relationship of trust is formed between the two parties. The secure ID system must protect this trusted relationship.

There are a number of factors that affect the real or perceived privacy of a secure ID system.

- ***Amount and type of personal information known and used by the ID system***. The more personal information the system needs to know and use, the higher the privacy concerns will be. For example, a system that needs to know and use an individual's name and mailing address will be considered less invasive to privacy than one that also requires a person's social security number and birth date. Confidentiality or sensitivity of the information is also a key consideration to privacy. A system that knows and uses sensitive information (for example, an individual's medical history) will likely cause greater concerns about privacy abuse than a system that only knows demographic data about its members. Biometric ID systems carry an added burden of knowing and using personal biometric information, which is widely regarded as being sensitive and private.
- ***Secure ID system architecture and technology***. There are a number of system design choices that can impact the privacy design of a secure ID system. Key considerations include location of private data (centrally in a database or locally on an ID card), how users of personal information are authenticated within the system, and how individual cardholders control access to personal information.

- ***Policies and practices used by the ID system to protect the use of personal information***. The secure ID system must be designed to protect personal information, restricting both access and use of the data to authorized persons and organizations. Protection of personal information is controlled both by the choice of system architecture and technology and the privacy policy and practices of the organization issuing IDs. A privacy policy must define the rules that the system agrees to abide by. For example, a system's privacy policy will include the rules that govern when and how a system can divulge information about its members. Privacy practices are the operational processes, systems, and people used to implement and enforce the ID system's privacy policy. A breakdown in privacy policy or practices often results in a rippling effect, reflecting badly on and raising doubt in other ID systems as well.

Example Applications

Figure 2 includes examples of the wide variety of uses for ID credentials that need a high level of security, privacy, and authentication for both the issuer and credential owner. As public acceptance and confidence in security technologies grow, smart cards, with biometrics, will be used in many of the applications below, keeping information separate and secure from attack threats.

Figure 2 - Example Applications

Physical Access	• Environment: campus, single building, parking lot • Interior: entrances, lobbies, offices, computer rooms, vaults • Transportation: buses, planes, trains, ships, subways
Logical Access	• Network: LAN, WAN, signed and encrypted e-mail, secure transactions • Common files: shared/working documents, employee handbook, newsletters • Confidential files: payroll, trade secrets, human resource files
Privileges	• Healthcare • Voting • Driver's license • Travel/border crossing • Electronic benefits
Law Enforcement	• Criminal records • Citizenship • Immigration status • User/document authenticity confirmation • Identification in time of death

What Are Biometrics?

Biometric technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics. Biometrics can provide very secure and convenient authentication for an individual since they cannot be stolen or forgotten and are very difficult to forge.

- A physiological characteristic is a relatively stable physical characteristic, such as an individual’s fingerprint, hand geometry, iris pattern, or blood vessel pattern on the back of the eye. This type of biometric measurement is usually unchanging and unalterable without significant duress to the individual.
- A behavioral characteristic is more a reflection of an individual’s psychological makeup. A signature is the most common behavioral biometric used for identification. Because most behavioral characteristics vary over time, an identification system using these must allow updates to enrolled biometric references.

Biometric System Components and Process

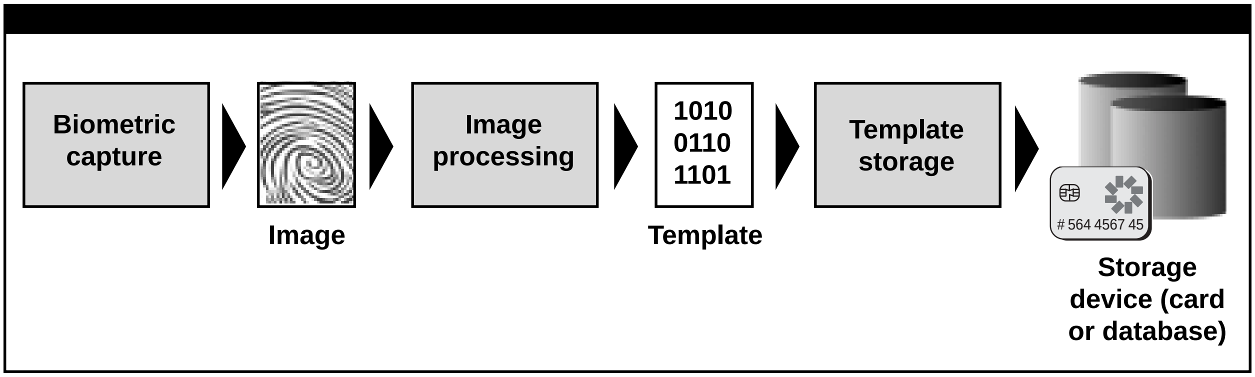
Three major components are usually present in a biometric system:

- A mechanism to scan and capture a digital or analog image of a living person’s biometric characteristic.
- Software for storing, processing and comparing the image.
- An interface with the applications system that will use the result to confirm an individual’s identity.

Two different stages are involved in the biometric system process - enrollment and verification.

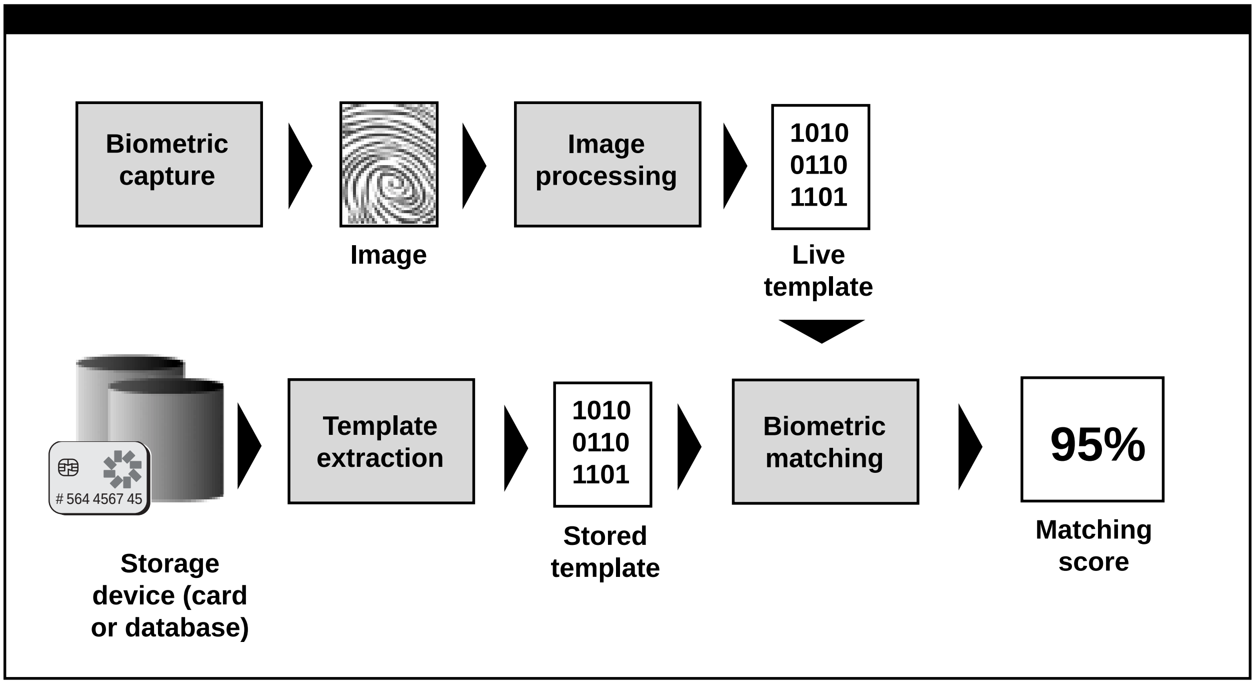
Enrollment. As shown in Figure 3, the biometric image of the individual is captured during the enrollment process (e.g., using a sensor for fingerprint, microphone for voice verification, camera for face recognition, scanner for eye scan). The unique characteristics are then extracted from the biometric image to create the user’s biometric template. This biometric template is stored in a database or on a machine-readable ID card for later use during an identity verification process.

Figure 3 - Example Enrollment Process



Verification. Figure 4 illustrates the identity verification process. The biometric image is again captured. The unique characteristics are extracted from the biometric image to create the user's "live" biometric template. This new template is then compared with the template previously stored and a numeric matching score is generated, based on the percentage of duplication between the live and stored template. System designers determine the threshold value for this identity verification score based upon the security requirements of the system.

Figure 4 - Example Verification Process



Secure identification systems use biometrics for two basic purposes: to identify or authenticate individuals.

Identification (1-to-many comparison) verifies if the individual exists within a known population. Identification confirms that the individual is not enrolled with another identity and is not on a predetermined list of prohibited persons. Identification will typically need a secured database containing a list of all applying individuals and their biometrics. The biometric for the individual being considered for enrollment would be compared against all stored biometrics. For many applications, an identification process is used only at the time of enrollment to verify that the individual is not already enrolled.

Authentication (1-to-1 comparison) confirms that the credential belongs to the individual presenting it. In this case, the device that performs the authentication must have access only to the individual's enrolled biometric template, which may be stored locally or centrally.

Selecting a Biometric Technology

The selection of the appropriate biometric technology will depend on a number of application-specific factors, including the environment in which the identity verification process is carried out, the user profile, requirements for verification accuracy and throughput, the overall system cost and capabilities, and cultural issues that could affect user acceptance. Figure 5 shows a comparison of different biometric technologies, with their performance rated against several metrics.

Figure 5 - Comparison of Biometric Technologies

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds
Accuracy	High	High	Very High	Very High	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Long-Term Stability	High	Medium	High	High	Medium	Medium	Medium

Source: "A Practical Guide to Biometric Security Technology," IT Professional, January/February 2001.[2]

A key factor in the selection of the appropriate biometric technology is its accuracy. When the live biometric template is compared to the stored biometric template, a matching score is used to confirm or deny the identity of the user. System designers set this numeric score to accommodate the desired level of accuracy for the system, as measured by the False Acceptance Rate (FAR) and False Rejection Rate (FRR). The False Acceptance Rate indicates the likelihood that a biometric system will incorrectly identify an individual or accept an impostor. The False Rejection Rate indicates the likelihood that a biometric system will reject the correct person. Biometric system administrators will tune system sensitivity to FAR and FRR to get to the desired level of accuracy supporting the system security requirements (e.g., for a high security environment, tuning to achieve a low FAR and tolerating a higher FRR).

Biometrics Resources

Additional information about biometric technology and standards can be found from the following organizations:

- The Biometric Consortium (www.biometrics.org).
- International Biometric Industry Association (www.ibia.org).
- BioAPI Consortium (www.bioapi.com).

Key Questions for a Combined Smart Card and Biometric ID System

A secure identification system combining both smart card and biometric technology can provide a very high level of confidence in the confirmation of an individual's identity, while also improving overall security and protecting the individual's privacy. There are several key questions to consider when designing the architecture of a secure ID system that will use both smart cards and biometrics.

Is the biometric system performing the Identification or Authentication process?

As discussed in the previous section, the identification process verifies if the individual exists within a known population by comparing their biometric data to those of other individuals stored in a secured database. This requires a 1-to-many comparison and may require substantial processing effort depending on the database size. More than one biometric may also be needed.   The authentication process confirms that an individual presenting an ID credential is its valid enrolled owner. This requires only a 1-to-1 comparison of live biometric data with previously stored biometric data. The following questions and discussion will focus on the use of smart cards and biometrics in the authentication process.

What biometric information is to be stored?

Either the complete biometric image or an extracted template of the biometric can be stored. Storing the complete biometric requires substantially more memory. For example, a complete fingerprint image will require 50 to 100 Kbytes, while a fingerprint template requires only 300 bytes to 2 Kbytes. The advantage of storing the complete biometric image is that the verification software and biometric algorithm can change from one match to the next. However, a much larger amount of memory on the ID credential is required, increasing the cost of the ID card. A system that captures and stores the complete biometric image may also present greater privacy concerns than one that stores a biometric template (from which it is impossible to extract the original biometric information).

Where is the biometric information stored?

Biometric data may be stored on the smart card, in the local reader, or in a central database. For a smart card based ID system, the biometric template would typically be stored in the smart card. This offers increased privacy and portability for the user and ensures the information is always with the cardholder, thus supporting offline processing. This design does require the smart card to have sufficient memory to store the appropriate biometric data. In some applications (such as door entry systems employing contactless smart cards with very little memory), the biometric template may be stored in the reader. This application would require that the smart card be used with a single reader, or where several access points exist, that the biometric database and readers be networked. Central database storage of biometric data may be considered to achieve a higher level of security (e.g., checking updated enrollment information) or to manage multiple types of readers that use the same biometric data but different algorithms.

Where is the biometric processing performed?

Biometric processing consists of two separate and sequential tasks. First, the user's "live" biometric template must be extracted and processed. Second, the live template must be compared with the trusted, stored template. The live biometric template extraction is a processor intensive task. A fingerprint extraction, for example, requires approximately 10 times more processing effort than a 1-to-1 fingerprint template comparison. In theory, both of these tasks may be performed in the smart card ID, in the reader, or on a central networked server. Smart card processors now exist that are capable of performing the biometric match, with processors currently in development that will be able to perform the live template extraction on the card itself. Smart card based ID systems support a private and secure biometric comparison process — extracting the live biometric template on the reader (with a relatively powerful microprocessor) and then transferring this template to the "trusted" smart card for comparison. The cardholder's stored biometric template never leaves the card and the matching is done within the card's secure processing environment. This system is commonly referred to as "match on card." Alternatively, all processing can be performed within a "trusted" reader if the ID cards have no or insufficient processing capability (e.g., crypto memory cards) or on a central server. One would only expect central processing to be chosen if the ID card and the reader had insufficient processing capability to handle the processing locally, or if additional security is required.

In conclusion, using smart cards with biometrics results in a trusted credential for verifying an individual's identity in a 1-to-1 authentication process. With the biometric template stored on the smart card, comparison can be made locally, without the need for an online reader. Due to storage requirements, most smart card technologies are more suited to storing biometric templates versus complete biometric images. Finally, with the latest secure smart card microcontrollers, sufficient on-card processing power and memory exists to perform the biometric match, providing a very private and secure identity verification system.

Smart Card Benefits in a Combined Smart Card/Biometric Identification System

Smart cards are widely acknowledged as one of the most secure and reliable forms of electronic identification. To provide the highest degree of confidence in identity verification, biometric technology is considered to be essential in a secure identification system design. This section summarizes the key benefits of a secure ID system that combines smart cards and biometrics.

Enhanced Privacy

Using smart cards significantly enhances privacy in biometric ID systems. The smart card provides the individual with a personal database, a personal firewall and a personal terminal. It secures personal information on the card, allowing the individual to control access to that information and removing the need for central database access during identity verification.

A Personal Database. How and where an ID system keeps personal information about its members is an important privacy consideration, affecting a system's real and perceived privacy behavior. Most ID systems store personal information for all system members in a central database. This centralization leads many to be concerned that their personal information is less protected, or at a minimum, more vulnerable to compromise. Smart cards store and safeguard personal information on the individual's card. The use of smart card IDs can promote confidence in an ID system by offering each member a unique secure, portable and personal database, separating their information from other members' data. With a smart card ID the cardholder maintains physical possession of private information. This enhances the trust relationship with the system, as the cardholder now shares in the decision of who is allowed to use their personal information for identity verification and in the responsibility to protect it.

The smart card personal database is portable and can be used in a variety of devices and networks. An ID system can take advantage of this portability by using closed local networks or standalone devices to carry out different identification tasks, rather than relying on a centralized system. By enabling local identity verification, smart card based secure ID systems can help alleviate concerns that the system is centrally tracking ID holder activities.

Unlike other ID card technologies that act as simple data containers, smart cards are unique in acting more like data servers, where data is not directly accessed but must be requested from the server (in this case the smart card's microprocessor). When used in combination with biometrics, a smart card ID becomes even more personal and private. A biometric provides a strong and unique binding between the cardholder and the personal database on the card, identifying the cardholder as the rightful owner of this card. The biometric cannot be borrowed, lost, or stolen like a PIN or password, and so strengthens the authentication of an individual's identity.

A Personal Firewall. In smart card based ID systems, the card is not just a data repository but also an intelligent guardian — a personal firewall — for the cardholder's information. When information is requested from the ID card, a smart card can verify that the requestor is authorized to perform such an inquiry.

A smart card ID also has the ability to behave differently based who is checking the ID. For example, most individuals will cooperate with a uniformed officer who requests to see an ID. But is this officer a valid officer? And what portion of the personal information is he or she authorized to see? With a smart card ID, the card would authenticate the officer through a portable card reader and release only the information that is relevant to the officer's responsibilities. The same ID card could be used to prove legal age when purchasing from a bar. In this case, the smart card ID would just confirm age, but not divulge any other personal information.

Once personal information is released, it is very hard to control what happens to the information, including how it might be used. It is an important privacy consideration for individuals to clearly understand when and to whom personal information is released by an ID system. The release of personal information is hard to control when carried out by a centralized database somewhere on a network, without the information owner's knowledge or consent. A smart card based ID system gives the cardholder control over who can access personal information stored on the card. A biometric further enhances this control, ensuring that only the rightful cardholder can authorize access to personal information.

A Personal Terminal. In today's electronic world, people often interact with systems through distributed or portable terminals. The authenticity and integrity of these terminals and the networks that connect them are important elements in protecting privacy. At their best, these terminals are secure agents of a trusted ID system, processing and protecting our personal information in a convenient and user-friendly fashion. At their worst, they can be Trojan horses, impersonating a valid system entry point while stealing private data.[3]

Because of their cryptographic processing capabilities, smart cards can be used in ID systems to increase the trustworthiness of terminals. This can translate into increased privacy for individuals and can allow cardholders to use anonymous devices as personal terminals. The increase in terminal trustworthiness is especially critical for biometric systems. Biometric ID systems rely on terminals to perform live-scan captures of some biometric trait. The ID system must be able to trust the biometric reader to capture and process a user's biometric. If it cannot, the integrity of the whole authentication process is compromised.

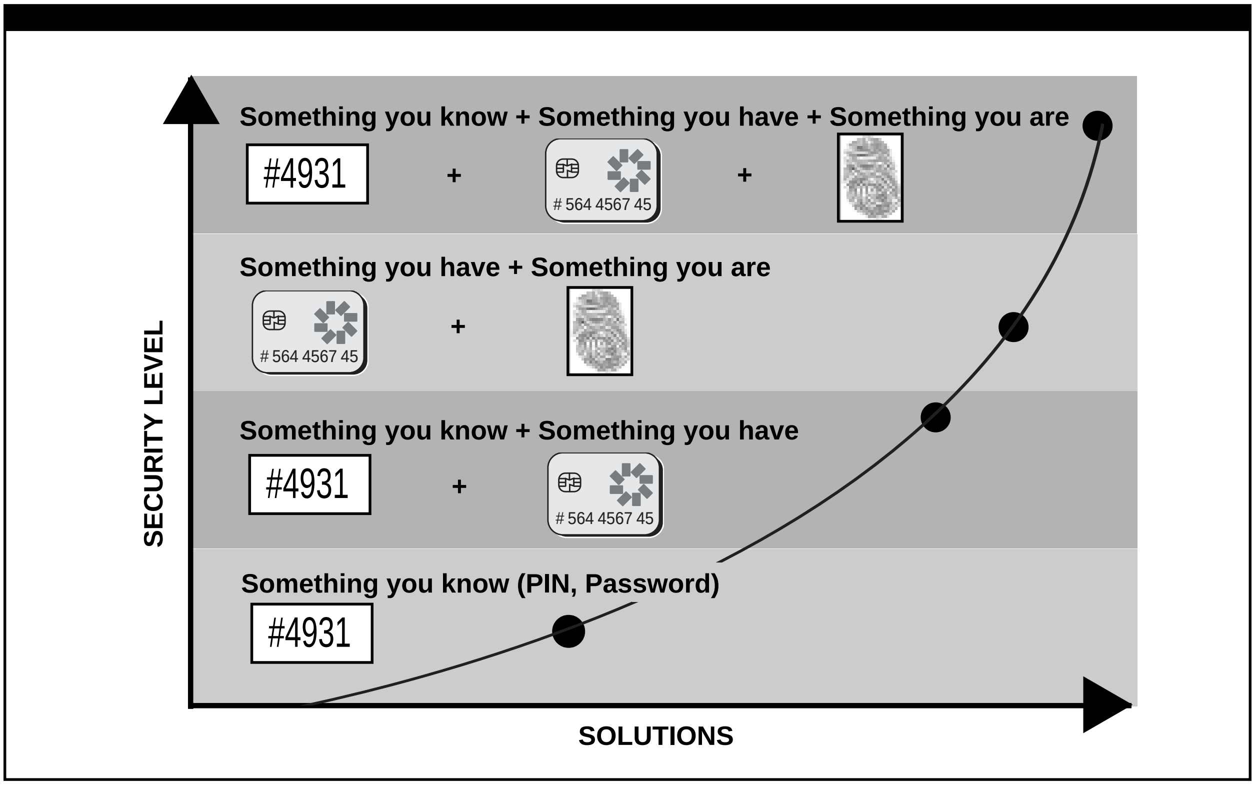
Smart cards can help to address this vulnerability. Using well-established security protocols, a smart card can participate in the exchange of digital certificates (or cryptographic secrets) with a terminal to determine its authenticity and trustworthiness. In essence, the smart card asks the terminal to prove that it is certified by the ID system. The terminal, in turn, asks the card to prove that it is a genuine member of the system. Once trust is established between the terminal and the smart card, it can then be extended to include the cardholder. By using biometric data captured from the cardholder at the point of use, the system can perform a match against enrollment data stored on the smart card. The ID system can thus authenticate that this user is the rightful owner of this card, and that the personal information stored on this card belongs to this cardholder. This process completes the trust relationship between the user, the card, the terminal being used, and the ID system.

In summary, smart cards and biometrics can help enable three important capabilities - a personal database, a personal firewall, and a personal terminal - that are useful in promoting and protecting the individual's privacy in ID systems. These features help the cardholder control who knows and uses personal information, how it is stored and protected, and who is trusted to see and use this data.

Enhanced Security

Biometric technologies are used with smart cards for ID system applications specifically due to their ability to identify people with minimal ambiguity. A biometric based ID allows for the verification of "who you claim to be" (information about the cardholder printed or stored in the card) based on "who you are" (the biometric information stored in the smart card), instead of, or possibly in addition to, checking "what you know" (such as a PIN). As shown in Figure 6, this increases the security of the overall ID system and improves the accuracy, speed, and control of cardholder authentication.

Figure 6 - Impact of Smart Cards and Biometrics on Security



As the importance of accurate identification grows, new technologies are being added to ID systems to improve their security. Figure 7 illustrates the features that smart cards and smart cards with biometrics provide to increase the overall security of an ID system. As discussed earlier, each ID application needs to determine the level of risk management required to counter security threats and then choose the level of technology appropriate for the desired level of assurance.

Figure 7 - Security Feature Summary

Smart Cards	Smart Cards with Biometrics
• Visual inspection of card for non-machine-read applications. • Automated inspection using readers. • Security markings and materials help thwart counterfeiting. • Integrated Circuit Chip (ICC) allows cryptographic functionalities to protect information and programs for multiple applications stored on the card. • Cryptographic co-processor on card allows protection of information stored in the chip, authentication of the trust level of the reader and establishment of secure communications. • High trust of information shared with the reader. • High security and strong user-to-card authentication.	• All attributes of smart cards. • Biometric templates are stored on the smart card ICC and are used to authenticate the cardholder, provide access to on-card data and enable the trusted terminal. • Counterfeiting attempts are reduced due to enrollment process that verifies identity and captures biometric. • Extremely high security and excellent user-to-card authentication.

An ID system using a contact or contactless smart card, cryptographic functions and biometrics has significant security advantages.

- The biometric template can be digitally signed and stored on the smart card at the time of enrollment and checked between the biometric capture device and the smart card itself each time the card is used.
- The template and other personal information stored on the cards can be encrypted to improve security against external attacks.
- Cardholder authentication can be performed by the smart card comparing the live template with the template stored in the card. The biometric template never leaves the card, protecting the information from being accessed during transmission and helping to address the user's privacy concerns.
- A smart card ID can authenticate its legitimacy, and that of the reader, by creating a mutually authenticated cryptographic challenge between the ID card and the reader before identity verification is started. Once that process has been accomplished, access to a specific application can be granted. This ensures a very high level of privacy for the cardholder, prevents inappropriate disclosure of sensitive data, and helps to thwart "skimming" of data that might be used for identity theft. The smart card ID can also challenge the biometric reader to ensure that a previously captured template is not being retransmitted in a form of playback attack.

- Smart cards have sufficient memory to store growing amounts of data including programs, one or more biometric templates, and multiple cryptographic keys to restrict data access and ensure that data is not modified, deleted, or appended.
- The smart card can also be used to prove the digital identity of its cardholder using cryptographic keys and algorithms stored in its protected memory, making smart cards ideal for applications that need both physical and logical authentication.

Improved System Performance and Availability

Storing the biometric template on a smart card also increases overall system performance and cardholder convenience by allowing local identity verification.

The identity of an individual is established and validated at the time the smart card is issued and the individual has proven eligibility to receive the identity card. From that point on, the user's identity is authenticated through the presentation of the smart card to a card reader, without the need to perform a search and match against a remote database over a network. This local processing can reduce the time to authenticate an individual's identity to one second or less, allowing faster security checks, and reduce the need for the card readers to be online with a central system.

The question may arise about how to handle a comparison failure (i.e., false rejection) without accessing a remote database. With smart card technology, it is straightforward for the security staff to revert to a visual comparison of a digitally signed, digitized photo or backup biometric also stored on the card.

For applications where fast and frequent use is necessary (e.g., controlling access to buildings and at airports), contactless smart cards can speed the transfer of biometric templates and eliminate the need to make a physical connection. Low cost, contactless smart cards with high communication speeds are now available that have enough memory to store a unique fingerprint template or photographic representation. This means higher security biometrics-based ID systems can use contactless smart cards to achieve a range of security, throughput and cost goals.

Improved Return on Investment

Using the combination of smart cards with biometrics for identification and authentication of individuals provides the most cost-effective implementation of a secure identification system.

Several ID and security technologies can be combined with a smart card, allowing deployment of different ID mechanisms based on the degree of security required and the budget available for implementation. Biometrics may be absolutely essential for those security checkpoints in the system where the user must be firmly linked to their ID card as the rightful owner and a password or PIN is not secure enough or lacks ease of use. Examples of systems requiring this stronger verification of identity include airport security gates or border crossings.

A government or corporate enterprise identification system may include a variety of physical and logical access checkpoints that have different levels of security requirements.   Biometric readers may be required at main entrances to the buildings, but internal access doors may only require the use of a magnetic stripe on the back of a smart card. When on a network, accessing different types of information may also have different security requirements. Some information may only require a password to access (which the smart card can store and remember for the user); other more sensitive information may require the use of a biometric; still other transactions may require the use of features on the smart card to digitally sign the transaction.

Contactless smart cards can be used in environments where high usage or environmental conditions are expected to affect the cost of maintaining the system. Because the contactless card chip and the reader communicate using radio waves, there is no need to physically make an electrical connection. Maintenance of readers is minimized while reliability is improved since there are no worn contacts to be replaced or openings to be unblocked. Cards also last longer because removing them from their regular carrying place is not necessary for use. Readers or kiosks can be sealed, allowing contactless ID systems to be deployed in almost any environment.

Smart cards uniquely provide a single device that can function as an individual's identity card and allow the combination of several technologies to cost-effectively address varying security needs of a system.

Upgradability and Flexibility

A key requirement for any identification system is the ability for the system to be upgraded without needing large investments in new infrastructure. For example, there may be a need to modify the system without replacing the individual ID cards if a security scheme is compromised or if enhanced capabilities become available. Because smart cards contain rewritable data storage, and in some cases rewritable program storage, they allow the most flexibility for updates to card data and card-system interaction algorithms and for secure management of multiple applications on a single card.

When used in biometric-based identity systems, a smart card ID can be upgraded, after issuance, as follows.

- Smart card IDs can have sufficient storage to upgrade or add new biometric content (e.g., new or different biometric templates).
- Some smart card IDs (those with EEPROM or flash memory for microprocessor program storage) can have on-card applications updated or new applications added as improved biometric algorithms are deployed.
- Smart card IDs can have on-card content partitioned into mutually private sections to be used by several different secure ID systems. For example, physical access activities and card content may be kept separate from transaction authentication activities and content. With a single multi-partition-capable identity card, new and private uses of the biometric content may be added to the card by any authorized issuing agency at any time.

This last capability makes use of another key smart card attribute - flexibility. Smart cards, due to their on-card processor and software, have the best ability to adapt to varying and evolving requirements.

- Their ability to be both securely read and written by authorized issuers adds system capabilities unavailable with other technologies.
- Their ability to actively detect tampering with information stored on the card is also unavailable except with smart cards.
- A smart card ID can support several biometrics: fingerprint, photographic facial image, retina or iris or hand geometry template, or any combination of these, simultaneously or incrementally over time.
- Smart card IDs may have both the traditional contact interface to reader/ writer mechanisms and a contactless interface for applications that require high throughput and usage without mechanical wear.
- The same physical smart card can contain multiple storage media, such as a printed photograph, printed bar code, magnetic stripe and/or optical stripe. Thus, a single card can be compatible with many forms of existing infrastructure.

In multi-application smart card IDs, each application can have its own degree of challenge and response activity depending upon the respective application's requirements. For example, a simple fingerprint comparison with the stored on-card template may be sufficient to authenticate a person's right to access certain premises, while the same card and fingerprint template may be used in conjunction with an encrypted digital signature exchange to authorize sensitive transaction rights.

In summary, the unique features of smart cards can deliver enhanced privacy, security, performance and return on investment to a secure ID system implementation. Their upgradability and flexibility for securely handling multiple applications and accommodating changing requirements over time are unmatched by other ID technology. Smart card technology, coupled with biometrics and privacy-sensitive architectures and card management processes, provides a proven, cost-effective foundation for a highly secure personal ID system.

Conclusion

A combined smart card and biometric ID system can significantly enhance cardholder trust in the system, while reducing risk for the ID card issuer. The authentication of the cardholder and the safe keeping of personal data on ID cards are substantially improved using smart cards with biometrics. Through the combination of the biometric information and on-card security functions, cardholder identity can be verified more accurately and securely.

While the combination of biometric and smart card technologies is only now starting to be implemented in secure ID programs, smart cards today provide the optimal implementation platform for a biometrics-based ID system. Smart cards can store the biometric templates, perform a local comparison and ensure that any network and reader communication is encrypted and authenticated. Smart cards also provide the unique capability to easily combine identification and authentication in both the physical and digital worlds.

The Smart Card Alliance urges organizations implementing secure ID programs to familiarize themselves with how the combination of smart card and biometric technology can deliver enhanced security, privacy, performance and return on investment.

For more information about smart cards and the role that they play in secure ID 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.

Endnotes

[1] "The Fight for Privacy Has Just Begun," BusinessWeek, Jan. 10, 2002 (www.businessweek.com/bwdaily/dnflash/jan2002/nf20020110_6472.htm)

[2] "A Practical Guide to Biometric Security Technology," by Simon Liu and Mark Silverman, IT Professional, January/February 2001 (www.computer.org/itpro/homepage/Jan_Feb/security3.htm)

[3] "ATM Theft," by Peter Ventura, SANS Institute, Nov. 22, 2000 (rr.sans.org/authentic/ATM_theft.php)

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, healthcare, 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.

Publication Acknowledgements

This white paper was developed by the Smart Card Alliance to discuss the combination of smart card and biometric technology in secure personal identification systems. 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 contributions. Members from more than 20 organizations, both public and private, were involved with the development of this white paper, including: ACI Worldwide, ADB, Atmel, Bank of America, Caradas, Cubic Transportation Systems, CrossCom National, Datacard Group, Datakey, EDS, Foley Hoag, Gemplus, IBM, Infineon Technologies, LaserCard Systems, MasterCard International, Northrop Grumman Information Technology, Oberthur Card Systems, Philips Semiconductors, SchlumbergerSema, and SCM Microsystems.

Special thanks go to those who wrote and reviewed this white paper.

Lead authors for the paper were:

Jeff Katz, Atmel
Gilles Lisimaque, Gemplus
Colleen Kulhanek, Datakey
Mark McGovern, EDS
John McKeon, IBM
Cathy Medich, Task Force Co-Chair
Gilles Pauzié, Gemplus
Joe Pilozzi, Philips Semiconductors
Martin Squibbs, Atmel

Task Force members who participated as contributing editors included:

Chuck Baggeroer, Datacard Group
Alan Bondzio, ADB
Lucien Dancanet, IBM
Oz Pieper, Consultant
Tate Preston, Datacard Group
James Russell, MasterCard International
Keith Saunders, MasterCard International
Louis Sciupac, LaserCard Systems
Michael Vermillion, EDS

Copyright Notice