Smart Cards and Biometrics

A Smart Card Alliance Physical Access Council White Paper

Publication Date: March 2011

Publication Number: PAC-11002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. 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. and Latin America. For more information please visit http://www.smartcardalliance.org.

TABLE OF CONTENTS

1 Foreword

This white paper is an update to the report, "Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems," first published by the Smart Card Alliance in 2002. The update was developed to:

- Incorporate updated information on biometrics technology and usage.
- Incorporate updated information on smart card technology and the benefits of combining smart cards with biometrics for identity verification.
- Showcase current case study examples of programs that combine biometrics and smart card technology.

2 Smart Card Technology and Biometrics

Smart card technology makes use of an embedded integrated circuit chip (ICC) that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The smart card connects to a reader with direct physical contact or with a remote contactless radio frequency (RF) interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption, mutual authentication and biometric matching) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, fobs, subscriber identity modules (SIMs) used in GSM mobile phones, ePassports, and USB-based tokens.[1]

There are two general categories of smart card technology – contact and contactless.

- A contact smart card must be inserted into a smart card reader with a direct connection to a conductive contact plate on the surface of the card (typically gold plated). Transmission of commands, data, and card status takes place over these physical contact points.
- A contactless smart card or device requires only close proximity to a reader. Both the reader and the card have antennas, and the two communicate using RF over this contactless link. Most contactless cards also derive power for the internal chip from this electromagnetic signal. The range is typically one-half to three inches for non-battery-powered cards, ideal for applications such as building entry and payment that require a very fast card interface.

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

- A biological characteristic is a relatively stable physical characteristic, such as an individual's fingerprint, hand geometry, iris pattern, facial shape and skin texture, or blood vessel pattern in the hand. This type of biometric trait is usually unchanging and unalterable without significant duress to the individual.
- A behavioral characteristic is more a reflection of an individual's psychological makeup. Speech patterns provide a method of speaker recognition and is the most common behavioral biometric used for verification. Another example of a behavioral biometric is dynamic signature verification. Because most behavioral characteristics vary over time, an identification or verification system using these must allow updates to enrolled biometric references.

2.1 Biometric System Components and Process

Four major components are usually present in a biometric system:

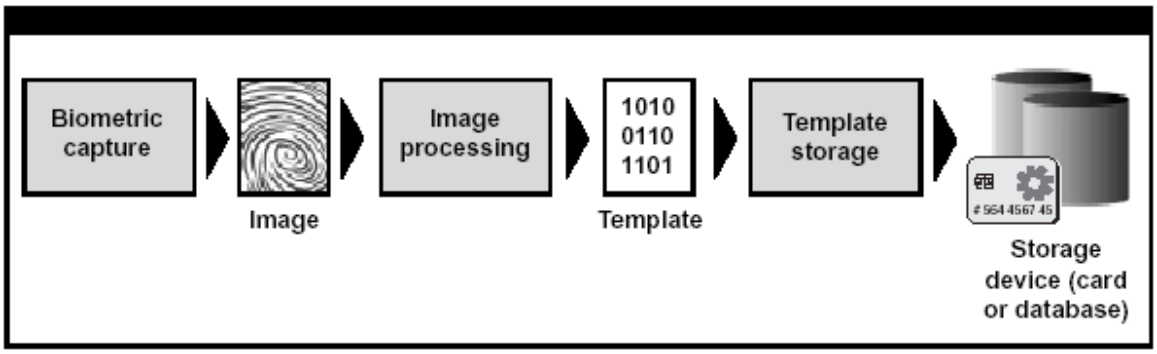
- A mechanism to scan and capture a digital representation of a living person's biometric characteristic.
- Software to process the raw data into a format (called a template) that can be used for storing and matching.
- Matching software to compare a previously stored biometric template with a template from a live sample.
- An interface with the application system to communicate the match result.

[1] While different form factors are available, for simplicity, this white paper refers to any device that uses smart card technology as a "smart card."

Two different stages are involved in the biometric system process – enrollment and matching.

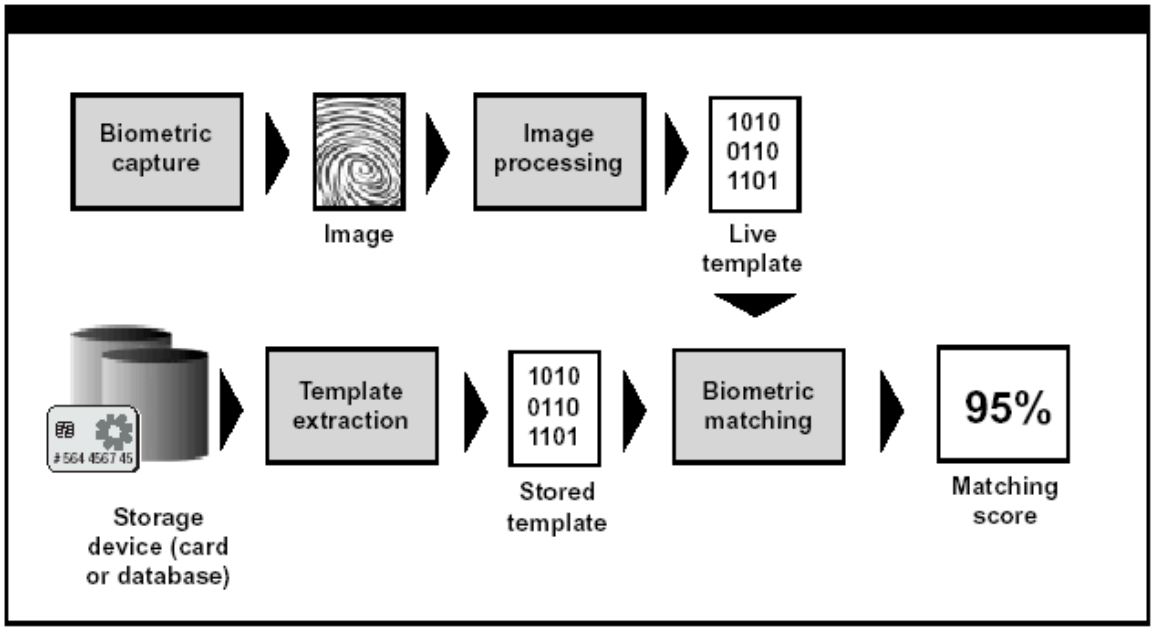
Enrollment. As shown in Figure 1, the biometric sample of the individual is captured during the enrollment process (e.g., using a sensor for fingerprint, microphone for speaker recognition, camera for face recognition, camera for iris recognition). The unique features are then extracted from the biometric sample (e.g., 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 a matching process.

Figure 1. Example Enrollment Process



Matching. Figure 2 illustrates the biometric matching process. The biometric sample is again captured. The unique features are extracted from the biometric sample to create the user's "live" biometric template. This new template is then compared with the template(s) previously stored and a numeric matching (similarity) score(s) is generated based on a determination of the common elements between the two templates. System designers determine the threshold value for this verification score based upon the security and convenience requirements of the system.

Figure 2. Example Matching Process



Biometrically-enabled security systems use biometrics for two basic purposes: identification and verification.

Identification (one-to-many or 1:N comparison) determines if the individual exists within an enrolled population by comparing the live sample template to all stored templates in the system. Identification can

confirm that the individual is not enrolled with another identity or is not on a predetermined list of prohibited persons. The biometric for the individual being considered for enrollment should be compared against all stored biometrics. For some credentialing applications, a biometric identification process is used at the time of enrollment to confirm that the individual is not already enrolled.

Verification (one-to-one or 1:1 comparison) determines whether the live biometric template matches with a specific enrolled template record. This requires that there be a "claim" of identity by the person seeking verification so that the specific enrolled template record can be accessed. An example would be presentation of a smart card credential and matching the live sample biometric template with the enrolled template stored in the smart card memory. Another example would be entry of a user name or ID number which would point to an enrolled template record in a database.

2.2 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 identification or verification process is carried out, the user profile, requirements for matching accuracy and throughput, the overall system cost and capabilities, and cultural issues that could affect user acceptance. Table 1 shows a comparison of different biometric technologies, with their performance rated against several metrics.

Table 1. Comparison of Biometric Technologies[2]

Biometric Identifier	Maturity	Accuracy	Uniqueness	Failure-to-Enroll Rate	Record Size (Bytes)	Universality	Durability
Face	M	M	M	L	H 84-2,000	H	M
Fingerprint (one print)	H	H	M	L-M	M 250-1,000	H	H
Hand	M	L	L	L	L 9	M	M
Iris	M	M	H	L	M 688	M	H
Signature	L	L	M	L	M 500-1,000	M	M
Vascular	M	M	H	L	M 512	H	H
Voice	L	L	M	M	H 1,500-3,000	H	L

Source: Report of the Defense Science Board Task Force on Defense Biometrics- March 2007

[2] High, medium and low are denoted by H, M, and L, respectively. Values assigned for the various qualities are subjective judgments, based on expert opinion and review of (several) current published sources.

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 (in a verification application), a similarity score is used to confirm or deny the identity of the user. System designers set the threshold (match or no match decision point) for this numeric score to accommodate the desired level of matching performance 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 verify 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 matching performance supporting the system security requirements (e.g., for a high security environment, tuning to achieve a low FAR and tolerating a higher FRR; for a high convenience environment, tuning to achieve a higher FAR and a lower FRR).

2.3 The Role of Smart Card Technology with Biometrics

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. Combining smart card technology with biometrics provides the means to create a positive binding of the smart card (a difficult-to-clone token) to the cardholder thereby enabling strong verification and authentication of the cardholder's identity.

2.3.1 Key Considerations for Implementing Combined Smart Card / Biometric Systems

2.3.1.1 Biometric Processing

Biometric processing consists of two separate and sequential tasks. First, the "live" biometric template of the user must be extracted and processed. Second, the live template must be compared with the trusted, stored template (i.e., performing the biometric match). The live biometric template extraction is a processor-intensive task. A fingerprint template extraction, for example, requires approximately 10 times more processing effort than a one-to-one fingerprint template comparison.

Smart card processors now exist that are capable of performing the biometric match, with processors in development that will be able to perform the live template extraction on the card itself. Two main smart card and biometric implementation approaches are "match-off-card" and "match-on-card."

- **Match-off-card**. For this type of implementation, the enrolled template is initially loaded onto the smart card and then transferred from the smart card via either contact or contactless interface when requested by the external biometric system. The external equipment then compares a new live template of the biometric with the one retrieved from the smart card. (The external equipment could be either the reader or a central computer system.) This implementation clearly has some security risks associated with transmitting the enrolled template off of the smart card for every biometric comparison. Appropriate security measures should be implemented to ensure the confidentiality and integrity of the released template. With this technique, the smart card is storing a template (or multiple templates), but has no significant knowledge of the type of biometric information, nor the ability to process it in any way. This implementation method is appropriate for all types of smart cards; this technique will work with memory, wired logic or microcontroller-based smart cards.
- **Match-on-card.** This implementation technique initially stores the enrollment template in the smart card's secure memory. When a biometric match is requested, the external equipment submits a new live template to the smart card. The smart card then performs the matching operation within its secure processor and securely communicates the result to the external equipment. This method protects the initial enrollment template since it is maintained within the smart card and never transmitted off-card. Cardholder privacy is also maintained with this technique since the cardholder's biometric template information is not readable from the smart

card. With this technique, the smart card must be a microcontroller-based device and be capable of computing the one-to-one comparison. Both smart cards and smart card readers are available that support match-on-card.

The National Institute of Standards and Technology (NIST) Minutiae Interoperability Exchange (MINEX) II program is dedicated to the evaluation and development of the capabilities of fingerprint minutiae matchers running on ISO/IEC 7816-compliant smart cards. The MINEX II test plan was released in February 2008. NIST conducted two rounds of public testing and released an updated test report on June 9, 2009. The final results of the most recent evaluation have been released as a revision of NIST Interagency Report (NISTIR) 7477[3].

2.3.1.2 Biometric Data

Either the raw biometric data (usually in the form of a bitmap image) or an extracted template of the biometric can be stored. For matching purposes, only the template is used. Storing the raw biometric data typically 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. Given the storage requirements, most smart card applications that use biometrics are based on template storage rather than image storage.

Some template formats are proprietary so there is a consideration for retaining the image in offline storage in the event that the template generation and matching software needs to change. If the images are retained, it is possible to generate new templates from the original images without requiring re-enrollment. Some biometric modalities, such as fingerprint, now support an interoperable template standard that works with template generation and matching software products provided by multiple vendors. The interoperability and performance characteristics for both proprietary and interoperable templates are reported in the NIST MINEX report.[4] In the case of iris recognition, non-proprietary interoperability is supported by storing a "compact image" format in applications (like those used with smart cards) with storage or bandwidth limitations. These compact formats support iris images usable for verification matching that are in the 2 to 4 Kbyte size range. Performance results of testing compact image formats are provided in NIST Iris Interoperability Exchange (IREX) test report[5].

2.3.1.3 Biometric Storage

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 matching without dependence on the availability of an online database connection. 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 or reader storage of biometric data may provide a higher level of throughput since the biometric data on the card does not have to be read.

2.3.1.4 Biometric Standards

A number of published standards relate to biometrics, including standards for data format, technical interfaces, application profiles, performance measurement and reporting. Standards are generally promulgated by recognized standards bodies. Within the U.S., the main standards work in biometrics is performed by the American National Standards Institute (ANSI)/International Committee for Information Technology Standards (INCITS) and NIST. ANSI's customary practice is to adopt International Organization for Standardization (ISO) standards as direct replacements to corresponding ANSI standards when such standards are approved by ISO for international use. Biometric standards can

[3] See link to NIST IR 7477 and other information about MINEX II testing at http://www.nist.gov/itl/iad/ig/minexii.cfm.
[4] NIST MINEX test program information can be accessed at http://www.nist.gov/itl/iad/ig/minex04.cfm.
[5] NIST IREX test program information can be accessed at http://www.nist.gov/itl/iad/ig/irex.cfm.

contribute to the success of system implementation where interoperability and choice of interchangeable vendor products are important considerations[6,7].

2.3.1.5 Multi-modal Biometrics

Some of the accuracy and usability limitations imposed by the use of a single biometric modality can be overcome by using multiple biometric modalities. Multi-modal biometrics enhance the overall matching accuracy through the use of multiple and independent biometric measurements. For example, the similarity score from a fingerprint measurement can be mathematically "fused" with an independent measurement of the vein pattern in the finger to yield a higher level of confidence in the identity of a person.

In addition, multi-modal biometrics can provide a solution for those individuals who are unable to present a suitable biometric sample in one modality. An example would be offering the option to present either a fingerprint or iris for authentication. A person who has poorly defined fingerprint patterns due to age, occupation, or medical condition would be given the choice to enroll and use iris as their biometric modality of choice. If both sensors are present, the user can use whatever modality that they are best suited for. In this situation, there is no fusion of independent biometric measurements.

As can be seen in Figure 3, multi-biometric systems can incorporate information from multiple modalities, instances, algorithms, sensors, samples, or any combination of the five[8]. Arguably, such systems may also include other sources of information, including biographic or travel document-based information.

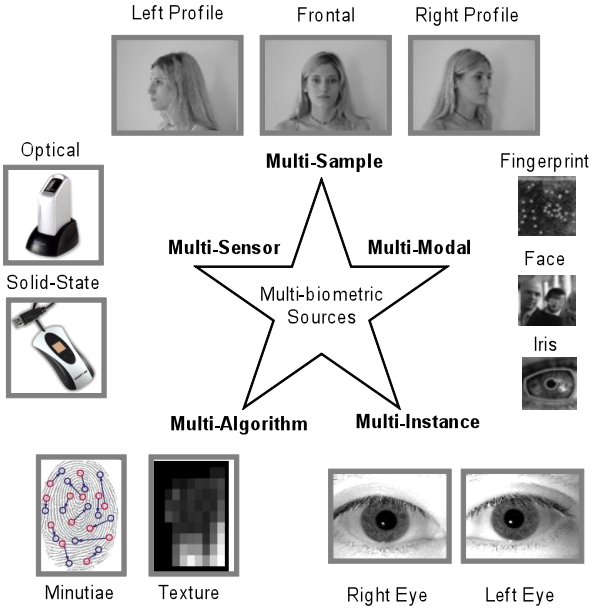


Figure 3. Multi-Biometric Source of Input

The trend toward multi-biometric systems has been particularly prevalent in large-scale U.S. government systems. The Department of Defense Automated Biometric Identification System (ABIS), Department of Homeland Security (DHS) Automated Biometric Identification System (IDENT), and Federal Bureau of Investigation (FBI) Next Generation Identification System (NGI) are all examples of systems which are

[6] A useful reference to biometric standards can be found at http://www.planetbiometrics.com/biometric-standards/.
[7] A summary of biometrics standards can be accessed at http://www.incits.org/tc_home/International_Standards_Published_as_of_09_08_2010.pdf.
[8] A. Ross, K. Nandakumar, and A. Jain, *Handbook of Multibiometrics*, Springer-Verlag New York, Inc., 2006.

currently multi-biometric in nature[9,10,11]. Furthermore, all three systems are increasing the number of biometric sources which can be leveraged.

2.3.2 Benefits of Combining Smart Card Technology and Biometrics

The combination of smart cards and biometrics delivers a number of significant benefits to organizations implementing secure identification system.

2.3.2.1 Enhanced Privacy

Using smart card technology 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 through advanced cryptography and digital signatures to prevent alteration or replacement of biometric data and to prevent cloning of the card. This allows the individual to control access to their biometric information and eliminates the need for central database access during identity verification.

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 a password, and so strengthens the authentication of an individual's identity.

A smart card-based ID system also 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.

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-sample captures of some biometric trait. The ID system should 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 card technology 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 completes the trust relationship between the user, the card, the terminal being used, and the ID system.

2.3.2.2 Enhanced Security

Biometric technologies are used with smart card technology 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 4, this increases the security of the overall ID system and improves the accuracy, speed, and control of cardholder authentication.

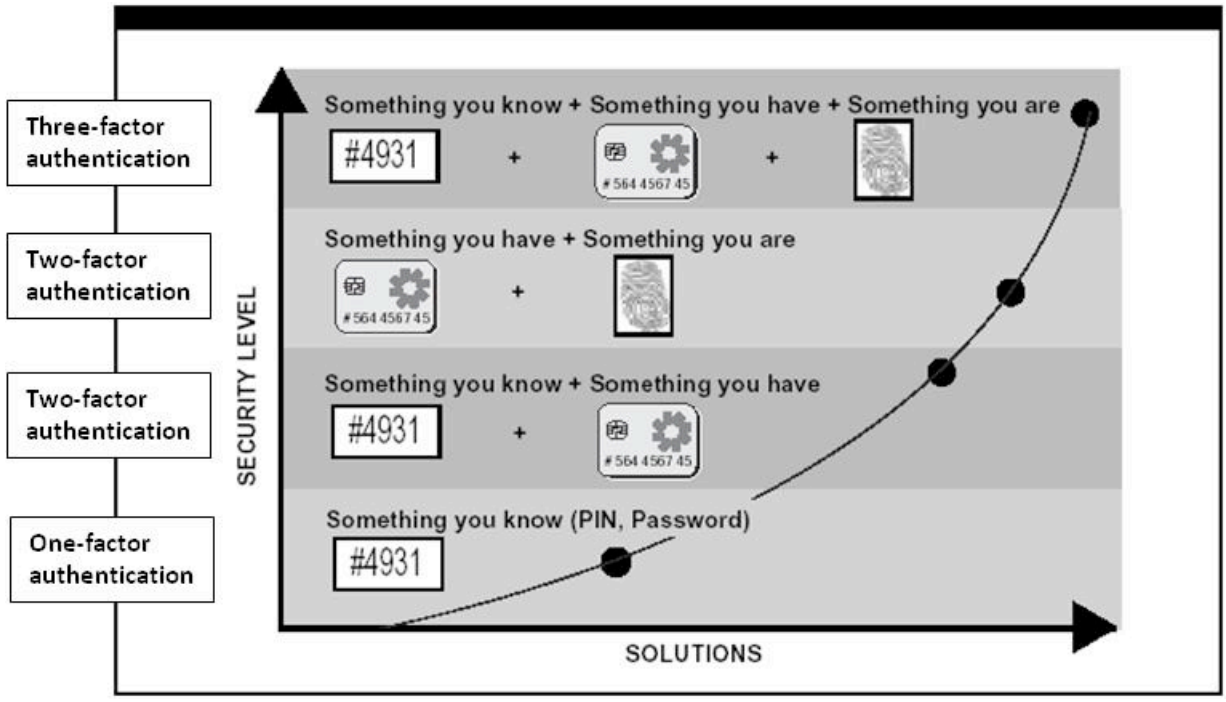
---

[9] "Next Generation ABIS Goes Operational, Now Referred To as DoD ABIS," DoD biometrics web site, January, 2009. http://www.biometrics.dod.mil/Newsletter/Issues/2009/Apr/v5issue2_a1.html.

[10] "Next Generation Identification," FBI web site, June 2009, http://www.fbi.gov/hq/cjisd/ngi.htm.

[11] "10-Fingerprint Scanners to Deploy at all Ports of Entry," DHS website, Nov. 2007, http://www.dhs.gov/files/programs/gc_1194553866460.shtm.

Figure 4. 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. Table 2 summarizes the features that smart card technology and smart cards with biometrics provide to increase the overall security of an ID system. 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.

Table 2. 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 to help thwart counterfeiting. • Integrated circuit chip (ICC), allowing cryptographic functionalities to protect information and programs for multiple applications stored on the card. • Cryptographic co-processor on card, allowing 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 stored on the smart card ICC 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 verification.

An ID system using contact or contactless smart card technology, 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 smart 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-based 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-based 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.

2.3.2.3 Improved System Performance and Availability

Storing the biometric template on a smart card 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 regarding 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. In the event of a false rejection, the cardholder can simply repeat the process.

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 card technology to achieve a range of security, throughput and cost goals. When biometric data is transmitted over a contactless interface between a smart card and a reader device, it is advised that the data transmission or data be encrypted to avoid any chance of unauthorized reading of the biometric data through eavesdropping or other surveillance methods.

2.3.2.4 Improved Efficiency

Using the combination of smart card technology with biometrics for identification and authentication of individuals provides the most efficient implementation of a secure authentication system.

Several ID and security technologies can be combined with a smart card, allowing deployment of different authentication 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 card technology 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; however, this may require the communication to be encrypted or, at least, not be able to be replayed. Maintenance of readers is minimized while reliability is improved since there are no worn contacts to be replaced or openings to be protected. 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.

2.3.2.5 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-based IDs can have sufficient storage to upgrade or add new biometric content (e.g., new or different biometric templates).
- Smart card-based 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 entity 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-based ID can support several biometrics: fingerprint, photographic facial image, iris, vascular or hand geometry template, or any combination of these, simultaneously or incrementally over time. Stored reference biometrics can also be updated as needed.
- Smart card-based 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-based 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 card technology 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.

3 Case Study Examples of Smart Card Technology Combined with Biometrics

This section includes brief case studies of identity verification systems that combine smart cards and biometrics.

3.1 Singapore Immigration Automated Clearance System

The Government of Singapore has implemented a smart card-based immigration self-clearance system using fingerprint biometric technology at 25 entry checkpoint locations around the island country. The system is called the Immigration Automated Clearance System (IACS) and is administered by the Singapore Immigration and Checkpoints Authority (ICA). The ICA is responsible for the security of Singapore's borders against the entry of undesirable persons and cargo through land, air and sea checkpoints. ICA also performs immigration and registration functions, such as issuing travel documents and identity cards to Singapore citizens, and issues immigration documents to foreign permanent residents.

The objective of the system is to provide an efficient and secure immigration clearance process at various entry points thereby allowing citizens to have "express" immigration clearance. Frequent travelers who wish to use IACS can apply for a personalized smart card which stores the cardholder's fingerprint data. When a citizen or foreign permanent resident cardholder enters Singapore, the card is inserted into a reader at a kiosk and the presented fingerprint is matched against the fingerprint data stored on the card. If the match fails, the traveler is directed to secondary screening. IACS has also been expanded to allow the use of machine-readable passports at the kiosks as long as the passport holder's fingerprints have been registered in the ICA database. This implementation is known as the Enhanced Immigration Automated Clearance System (eIACS).

IACS has been implemented at two major land entry points that connect to Singapore via causeway from Malaysia. These entry points handle large volumes of bus, car and motorcycle travelers. In addition, IACS checkpoints are placed at airport terminals, cruise terminals, ferry terminals, and other port facilities. In 2009, the ICA processed 74 million arriving passengers. The ICA issues about 100,000 ID smart cards and 500,000 passports each year. More information on the system is available on the ICA web site at http://www.ica.gov.sg/page.aspx?pageid=196.

3.2 Canadian Airport Restricted Area Identification Card

In 2004, the Canadian Air Transport Security Authority (CATSA) was assigned responsibility to develop a Restricted Area Identification Card (RAIC) program for airport employees at the 29 major Canadian airports. RAIC is designed to allow individual airports to control where users may access restricted areas and to enhance security during heightened threat levels. The RAIC is a biometrically-enabled HID iClass® smart card that is designed for use by airport workers seeking entry to restricted areas through automated or guarded access portals and vehicle gates. The RAIC is also read using portable readers at pre-board screening areas to validate employee identity and credentials prior to screening.

Applicants must first complete a security clearance screening process conducted by Transport Canada, including submitting biographical data and fingerprinting for a criminal record check and national security check. Once an applicant has successfully completed the background screening process, Transport Canada will issue a Document Control Number and CATSA will approve the issuance of the RAIC. The airport conducts the enrollment process and generates the RAIC with embedded biometrics and a unique identification number. Fingerprint and iris biometric data are collected from the applicant along with biographical data and the applicant's facial photo. CATSA chose to store the biometric data on the smart card as opposed to a database option. The smart card has an embedded chip with a contactless interface, a variable data strip, a magnetic strip and physical security features. As a result, many existing airport functions can be combined on a single card.

RAIC allows users working at multiple airports and aircrew personnel to use a common biometric identity system to enhance national security. Transport Canada and CATSA manage a centralized database allowing real-time management and revocation of RAICs. Airports receive real-time notification from CATSA if an RAIC is cancelled or revoked and can remove the user from their local physical access control system (PACS) to deny access. It should be noted that the airport authority controls user access to restricted areas. More than 100,000 Canadian airport employees are enrolled in the RAIC program and RAIC is implemented across 29 Canadian airports. Because this is a "closed" system, the biometric template data stored on the RAIC can be in the proprietary template form. While this supports a level of interoperability among locations, it is not the same as "open" interoperability achieved when using interoperable standard templates.

It should be noted that a number of U.S. airports have also implemented biometrics and smart card technology for physical access to restricted areas. Examples include San Francisco International Airport, Chicago O'Hare Airport, and Seattle-Tacoma International Airport.

3.3 Amsterdam Schiphol Airport

Schiphol Airport in Amsterdam, Netherlands, pioneered the use of iris recognition in the airport environment. Long before the post 9/11-security frenzy, Schiphol planned for biometric-based access control to secure restricted areas within the airport environment, ensure efficient airport operations, and comply with all appropriate regulations by the most cost-effective means possible. Not only did Schiphol's operators want to improve security, they wanted to improve the user security experience as well. Accurate, reliable, and quick-and-easy identification and authentication were considered critical to meeting these objectives. Iris recognition was selected as the access control biometric modality of choice in the process re-engineering employed to streamline, automate, and optimize staff badging and credentialing at Schiphol Airport.

Schiphol's workforce includes 60,000 airport workers employed by more than 500 companies. The goals of the iris-based biometric access control system were to: 1) prevent transferability of access cards and PINs; 2) reduce errors associated with the "human" identification processes; 3) automate security functions to the greatest extent possible; and 4) increase user convenience. In addition, stringent privacy policies were applied. These policies included matching of the biometric on a smart card with no centralized template storage, overt user participation (e.g., no distance or surveillance iris capture), built-in identity theft protection, encrypted data storage on the smart card and in the communication between the card and readers to prevent skimming, and use of private, highly secure keys.

The access control solution at Schiphol relies on a unique combination of iris recognition and weight measurement to access and pass through a "mantrap" portal. The authorization to open the first door is based on validation of the smart card and verification of the iris pattern on the card with the cardholder. A second iris verification along with weight measurement (obtained via a scale embedded in the portal) opens the second door.

The access control system at Schiphol went live in 2004 and became fully operational in 2006. Today, Schiphol processes 60,000 accesses per day across 110 access control points with an average throughput of eight seconds and a rejection rate of less than one percent. As a result, Schiphol has experienced improved accuracy of verification over the previous system and extremely high user acceptance of this contactless, hygienic, and rapid access control solution.

3.4 University of Arizona Keyless Access Security System

The University of Arizona (U of A) located in Tucson, Arizona, USA, is a public research university serving the citizens of Arizona and beyond. The mission of U of A is to provide a comprehensive, high-quality education that engages its students in discovery through research and broad-based scholarship. Founded in 1885, U of A has 37,000 undergraduate, graduate, professional and medical students and 12,000 employees.

The U of A has established a campus-wide unified Keyless Access and Security System Program to better manage its resources and facilities. This system allows the use of a biometric contactless smart

card called the “CatCard” for access to university facilities by students, faculty, staff, and affiliates. The focus of the system is to address the issues of loss prevention and personal safety and to provide convenience through the use of standardized technology. The system was launched in 2006 as an optimized one-card concept to replace several independent access control systems installed on the U of A campus. The system is supported by comprehensive policy and standards so that it is uniformly integrated with all new construction, remodeling or other building programs. The system includes a computerized control center to manage, process, record, and notify appropriate response agencies as needed. The CatCard is the official University of Arizona identification card.

The card features a digitized photo, digitized signature, contactless smart chip, and magnetic stripe. Today there are approximately 800 door access readers, of which 215 utilize contactless smart chip technology. 75,000 active cardholders use their CatCards at 182 facilities to gain access to a variety of buildings, labs and general use areas that would have required the issuance of keys in the past. Along with reducing the number of keys issued, a comprehensive audit trail is available to review access transaction history by authorized management personnel. The U of A has established standardized incident response protocols to allow the University of Arizona Police Department (UAPD) to respond to a specific location rather than a general building location. The system is also integrated with digital video security cameras throughout the campus to allow UAPD to observe various locations in real-time directly from the UAPD dispatch center. This also provides an easy audit trail of historical information for later use.

According to the U of A, one of the benefits of using a contactless smart card is that it reduces wear and tear on the card and minimizes the cost of replacing worn or damaged cards. To protect cardholder privacy, the student or employee ID number is not printed on the surface of the CatCard. Instead, a randomly assigned 16-digit unique identifier (called the ISO number) is used to identify all cardholders. This unique identifier facilitates services associated with the CatCard.

A contactless smart chip is embedded into the CatCard. It is a multi-application chip that has the capability to store a prepaid value directly on the card as well as biometric data. Photos and signatures are stored in the card management system, and fingerprint template data is obtained during enrollment and stored digitally on the card. The photo and signature are also printed on the face of the CatCard for identification purposes. Digital storage of this information in the card management system allows efficient and quick card replacement in case a card is ever lost, damaged or stolen, and provides an additional means to identify persons requesting replacement cards.

In addition to physical access to facilities, the CatCard has the following uses:

- Bursar (financial) account authorization
- Prepaid purchase of printing and copying
- Library privileges
- Campus recreation center access
- Prepaid parking and transportation services
- Identification and status verification
- U of A athletics pass verification
- Meal plans
- Automated teller machine (ATM) access and PIN-based debit purchase[12]

Fingerprint biometric data stored on the card is verified against the presented biometric of the cardholder for access to high security/high risk facilities.

3.5 U.S. FIPS 201 Personal Identity Verification (PIV) Card

In August 2004, President George W. Bush issued the Homeland Security Presidential Directive 12 (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors,” which

[12] These services are available when the CatCard is linked to a Wells Fargo Bank checking account.

directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. This standard applies to identification issued by Federal departments and agencies to Federal employees and contractors for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems (except for national security systems). HSPD-12 further specifies secure and reliable identification that:

- Is issued based on sound criteria for verifying an individual employee's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.

Information for both Federal employees and contractors is held on a Personal Identity Verification (PIV) card. The PIV card is personalized with identity information for the individual to whom the card is issued. It allows identity verification to be performed by both humans and automated systems. Humans can use the physical card for visual comparison, whereas automated systems can use the electronically stored data on the card to conduct automated identity verification. The PIV card's smart card chip stores personal information, including biometric data. (It is best practice to digitally sign biometric data to prevent fraudulent tampering with or replacement of the biometric identifier.) When the smart card is inserted into a contact reader and a PIN is entered, the cardholder's fingerprint will be matched with the fingerprint template stored on the PIV card. If the match is verified, the system gives the cardholder access to Federal buildings or networks (if logging on to a computer), depending on the access privileges that have been assigned to that person.

As of September 1, 2010, the White House reported that 3,536,315 PIV cards have been provided for Federal employees and 1,062,201 PIV cards have been issued to contractors and others requiring access.[13]

3.6 U.S. Department of Defense Common Access Card

The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as standard identification for active duty military personnel, selected reserve personnel, DoD civilian employees, eligible contractor personnel, eligible Federal personnel, and other DoD-sponsored eligible populations. The CAC is used in several ways, including as a general identification card, for authentication to access DoD computers, networks, and certain DoD facilities, as well as serving as an identification card under the Geneva Conventions. The CAC enables encrypting and cryptographically signing email, facilitates the use of public key infrastructure (PKI) authentication tools, and establishes an authoritative process for the use of identity credentials.

As of 2008, approximately 3.5 million active CACs were in circulation. DoD has deployed an issuance infrastructure at over 1,000 sites in more than 25 countries around the world and is rolling out more than 1 million card readers and associated middleware. In compliance with HSPD-12, the DoD began issuing its next-generation CAC in October, 2006. Pursuant to the President's mandate, the new HSPD-12 compliant card contains advanced technology (including biometrics), which enhances the security of Federally controlled facilities and computer systems.

To receive a next-generation CAC, all eligible personnel must be entered into the Defense Enrollment Eligibility Reporting System (DEERS). To establish a DEERS record, all personnel must undergo proper identity vetting. Once vetted the applicant makes an appointment with a Real-Time Automated Personnel Identification System (RAPIDS) operator and provides two forms of identification to authenticate identity. Both IDs must be among those listed on the I-9 Form; one must bear a photo (e.g., passport, driver's license). A current/unexpired CAC is considered a valid form of ID. During enrollment, the RAPIDS operator confirms the applicant's identity and the applicant provides fingerprints and facial photograph, and creates a PIN to use with the card.

[13] Current status of PIV card issuance can be found at http://www.whitehouse.gov/omb/e-gov/hspd12_reports/.

3.7 U.S. Transportation Worker Identification Credential (TWIC)

The Transportation Worker Identification Credential (TWIC) is a tamper-resistant biometrically-enabled smart card that is issued to all transportation workers that require unescorted access to secure areas of U.S. regulated maritime facilities and vessels. These populations include but are not limited to:

- Non-credentialed mariners in vessel crew
- Longshoremen
- Facility employees who work in a secure area
- Drayage truckers
- Truckers bringing/picking up cargo at a facility
- Surveyors
- Agents
- Chandlers
- Port chaplains
- Other maritime professionals

TWIC was established by the U.S. Congress through the Maritime Transportation Security Act (MTSA) and is jointly administered by the Transportation Security Administration (TSA) and U.S. Coast Guard. The TWIC program began enrollment and issuance at the Port of Delaware in October, 2007. The TWIC program was established in response to identity management threats and vulnerabilities identified in the U.S. transportation system. Threat examples include the following:

- Inability to positively identify individuals who seek to gain unescorted access to secure areas of the transportation system.
- Inability to assess the threat posed to the transportation system by those who seek or have unescorted access to secure areas of the transportation system due to a lack of background information, or the lack of uniformly determined background information.
- Inability to protect current worker credentials against fraud.

The TWIC process requires that the identity of each TWIC applicant has been verified, that a security threat assessment has been completed on that identity, and that each credential issued is linked to the rightful holder through the use of biometric technology. Local maritime facility and vessel operators may then choose to grant access to those persons who have been issued a valid TWIC.

Each applicant for a TWIC must provide biographic information, identity documents, and biometric information (i.e., fingerprints), sit for a digital photograph, and pay the established TWIC fee. TSA sends pertinent parts of the enrollment record to the FBI, as well as within DHS, so that appropriate terrorist threat, criminal history, and immigration checks can be performed. TSA reviews the results of the checks to determine if the person poses a security threat and notifies the applicant of the results. When TSA determines that an applicant qualifies to receive a TWIC, a credential is produced and sent to the enrollment center at which the applicant applied. The applicant must return to the enrollment center for issuance and activation of the TWIC. Possession of a TWIC does not guarantee access to secure areas because the owner/operator controls which individuals are granted unescorted access to the facility or vessel. Rather, the TWIC is a secure, verified credential that can be used in conjunction with the owner/operator's risk-based security program that is required in security regulations issued by the Coast Guard.

At this writing, TSA was in the process of completing a series of field pilot tests of TWIC biometric and card reader devices (both fixed and handheld) at several major port facilities across the U.S. This pilot test will measure the impact on commercial maritime operations when using the TWIC card for automated access control as well as test the performance of the technology in the challenging maritime environment. It is expected that the U.S. Coast Guard will issue regulations requiring use of TWIC readers by the end of 2012. As of January 1, 2011, over 1.7 million TWIC cards have been activated and issued.

3.8 Electronic Passports

The electronic passport, or ePassport, is the same as a traditional passport book with the addition of a small, embedded integrated circuit (i.e., smart card chip). In the United States and many other countries, the chip is embedded in the back cover. The chip stores:

- The same data visually displayed on the data page of the passport
- The passport holder facial image photo stored in digital form
- The unique chip identification number
- A digital signature to detect data alteration and verify signing authority
- Additional data, as defined by specific issuing governments

Standards for the ePassport have been established by the International Civil Aviation Organization (ICAO) and are followed by all countries implementing ePassports. All ePassports can be recognized by an internationally recognized symbol that is printed on the front cover. This electronic passport symbol identifies the passport as an ePassport. The symbol is also displayed at border crossing stations that have the capability to process ePassports.

All ePassports follow the common ICAO standard. However, countries implement ePassport programs according to their specific policies and may implement different options specified in the standard including the addition of fingerprint and iris biometric identifiers. This results in differences among country implementations of ePassports even though they all conform to the ICAO specification.

Extended Access Control (EAC) is the additional security access mechanism defined in the ICAO ePassport specification to meet data protection requirements and to help protect the privacy of additional biometric data (for example, fingerprints and iris identifiers). Implementation is planned in future generations of ePassports and will be country-specific. EAC also ensures that access to biometric data is only possible if allowed by the issuing country. EAC uses additional cryptographic mechanisms to protect biometric data from being retrieved without proper authorization. An ePassport equipped with EAC protects the additional biometric data using encryption. Each ePassport will have unique keys to protect access to the sensitive information. With the help of EAC, ePassport readers at ports of entry can be authorized to read data, and selective access rights can be defined. The retrieval of fingerprints requires sovereign powers (e.g., the permission of the country which issued the ePassport). EAC makes it possible to define whether an authorized entity is able to access the additional information.

The following is a list of countries who currently issue or have plans to issue EAC ePassports: Albania, Armenia, Australia, Bosnia and Herzegovina, Brunei, Canada, Croatia, Dominican Republic, Iran, Iraq, Malaysia, Sovereign Military Order of Malta, Moldova, Montenegro, Morocco, New Zealand, Nigeria, Singapore, Switzerland, Tajikistan, Thailand, Turkey, Turkmenistan, and Venezuela.

4 Conclusions

In conclusion, using smart cards with biometrics results in a trusted credential for authenticating an individual's identity using one-to-one biometric verification. With the biometric template stored on the smart card, comparison can be made locally, without the need for connection to a database of biometric identifiers. Since all biometric matching takes place using templates, it is unnecessary to store complete biometric image data on the smart card. With the latest secure smart card microcontrollers, sufficient on-card processing power and memory exist to perform the biometric match directly within the logic of the smart card instead of within the reader device. This biometric match-on-card approach can provide an even more private and secure identity verification system.

5 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Physical Access Council to describe the benefits of combining smart cards and biometrics to enable strong verification and authentication of an individual's identity. The document is an update to a 2002 white paper, with new information added on biometrics technology and use cases that combine smart cards and biometrics in identity programs.

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 thanks the Council members for their contributions. Participants involved in the development of this white paper update included: AMAG Technology; Bioscrypt/L-1 Identity Solutions; Booz Allen Hamilton; CSC; Datacard Group; Datawatch; Diebold; General Services Administration (GSA); HID Global; Hirsch Electronics; HP; IDenticard; Identification Technology Partners; IDmachines; Intellisoft, Inc.; NagraID Security; NASA; Probaris, Inc.; Roehr Consulting; SCM Microsystems; Software House/Tyco; U.S. Department of Defense/Defense Manpower Data Center (DMDC); U.S. Department of State; XTec, Inc.

Special thanks go to **Walter Hamilton**, Identification Technology Partners, who managed the project, and to the following individuals who contributed content or participated in the development and review of this updated document:

- **Dave Adams**, HID Global
- **Tim Baker**, Identification Technology Partners
- **Salvatore D'Agostino**, IDmachines
- **Tony Damalas**, Diebold
- **Tony Ferguson**, Bioscrypt/L-1 Identity Solutions
- **Marty Frary**, Consultant
- **Marlon Guarino**, DMDC
- **Walter Hamilton**, Identification Technology Partners
- **Jean Henaff**, Datacard Group
- **Daryl Hendricks**, GSA
- **Won Jun**, Identification Technology Partners
- **Lolie Kull**, HP
- **Rick Lazarick**, CSC
- **LaChelle LeVan**, Probaris
- **Gilles Lisimaque**, Identification Technology Partners
- **Diana Loughner**, IDenticard
- **Stafford Mahfouz**, Software House/Tyco
- **Don Malloy**, NagraID Security
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, SCM Microsystems
- **Tim Meyerhoff**, IrisID
- **David Nichols**, HID Global
- **Zeca Pires**, Datacard Group
- **Rick Pratt**, XTec, Inc.
- **Kenny Reed**, Datawatch
- **Roger Roehr**, Roehr Consulting
- **Steve Rogers**, Intellisoft, Inc.
- **Jason Rosen**, NASA
- **Dan Schleifer**, IDmachines
- **Adam Shane**, AMAG Technology
- **Mike Sulak**, U.S. Dept. of State
- **Lars Suneborn**, Hirsch Electronics
- **Abel Sussman**, Booz Allen Hamilton
- **Rob Zivney**, Hirsch Electronics

Individuals who participated in the development and review of the first version of this white paper, published in May, 2002, included: Chuck Baggeroer, Datacard Group; Alan Bondzio, ADB; Lucien Dancanet, IBM; Jeff Katz, Atmel Corporation; Colleen Kulhanek, Datakey; Gilles Lisimaque, Gemplus: Mark McGovern, EDS; John McKeon, IBM; Gilles Pauzie, Gemplus; Oz Pieper, Consultant; Joe Pilozzi, Philips Semiconductors; Tate Preston, Datacard Group; James Russell, MasterCard; Keith Saunders, MasterCard; Louis Sciupac, LaserCard Systems; Martin Squibbs, Atmel Corporation; Michael Vermillion, EDS.

About the Physical Access Council

The Smart Card Alliance Physical Access Council is focused on accelerating widespread acceptance, use, and application of smart card technology for physical access control. The Council brings together leading users and technologists from both the public and private sectors in an open forum and works on activities that are important to the physical access industry and address key issues that end user organizations have in deploying new physical access system technology. The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software, and reader vendors; physical access control system vendors; and integration service providers.

6 Appendix A: *Key Questions for a Combined Smart Card and Biometrics Identification System*

A secure identification system that combines both smart card and biometric technology can provide a very high level of confidence in confirming an individual's identity while also improving overall security and protecting the individual's privacy. Several key questions should be considered when designing the architecture of a secure ID system that will use both smart cards and biometrics.

Is the biometric system performing an identification or verification process?

As discussed in the white paper, the identification process determines 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 one-to-many comparison and may require substantial processing effort depending on the database size. More than one biometric modality may also be needed. The verification process confirms that an individual presenting an ID credential is its valid enrolled owner. This requires only a one-to-one 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 verification 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 on the smart card. For example, a complete fingerprint image will require 50 to 100 Kbytes, while a fingerprint template requires only a few hundred bytes. The advantage of storing the complete biometric image is that the verification software and biometric algorithm can be changed without requiring the user to re-enroll their biometric sample. 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 which is a processed derivative of 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 secure memory of the smart card. This offers increased privacy and portability for the user and ensures that the information is always with the cardholder, thus supporting offline processing and eliminating the need for access to online databases. Biometric data stored in the memory of a smart card can be further protected from unauthorized access by using cryptographic means and digitally signing the biometric template to prevent alteration or replacement.

Where is biometric processing performed?

Biometric processing consists of two separate and sequential tasks. First, the raw biometric data from the presented "live" sample be processed using a feature extraction algorithm to produce a template. Second, this template must be compared with the stored template. Template extraction is a processor-intensive task. For example, a fingerprint template extraction requires approximately ten times more processing effort than a one-to-one fingerprint template match comparison. In theory, both of these tasks may be performed in the smart card (match-on-card), in the reader (match-on-reader), or on a central networked server (match-on-server). Smart card-based ID systems now support the most 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 matching on the card. The cardholder's stored biometric template never leaves the card and the matching is done within the card's secure processing environment. Alternatively, all processing can be performed within a "trusted" reader if the ID cards have no or insufficient processing capability (e.g., if using cryptographic 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.

Is biometric matching accurate?

Although matching errors can occur, most biometric technologies today are very accurate. A biometric match decision is based on a similarity score that is compared against a threshold setting. If the score exceeds the threshold, the system concludes that there is a match. Conversely, if the similarity score is less than the threshold setting, the system reports that the comparison is not a match. Depending on the characteristics of the system, the threshold setting can be configured to be more or less secure. A higher security setting will result in more frequent occurrence of false rejections. In such a case, the user must repeat the biometric presentation which is usually just a minor inconvenience. Conversely, a less secure threshold setting may increase the chance of an imposter gaining access. While a random imposter attempt may be statistically feasible, even the least secure threshold settings would typically result in only a 1% probability of a successful match. If a hacker knew that there was a likelihood that a random attempt would fail 99% of the time, they would likely choose another point of attack within the system.

One of the largest biometrically-enabled smart card ID systems is the Personal Identity Verification (PIV) card for U.S. Federal workers and contractors. NIST has tested and certified a number of standards-based fingerprint feature extraction and matching algorithms for use in the PIV card; the algorithms are listed on the NIST web site. Each of these manufacturers has been shown to meet the government standard of 99% matching accuracy (where the combination of false rejections and false matches are less than or equal to 1%). This standard is even more impressive when you consider that the PIV card is used in an interoperable environment where enrollment and matching might use different manufacturers' technology. Proprietary technologies that do not require interoperability are typically even more accurate. When you consider the uncertainties that exist in other authentication technologies like passwords and PINs that can be forgotten, guessed or hacked, biometric matching accuracy compares favorably.

Can a biometric sensor be spoofed by using a fake biometric sample?

The susceptibility of biometric sensors to a “spoofing” attack varies among different manufacturers. Today, many biometric sensor manufacturers are incorporating features that can detect “liveness” of the presented biometric sample. Consideration should be given to implementing these “spoofing” countermeasures – particularly if the biometric presentation is performed in an unattended environment. Examples of such spoofing attacks include the use of fake fingers made of various materials like rubber, silicone, gelatin, wax, or plastic; use of photographs of an iris or face; or other methods to fool the sensor into thinking that the sample is coming from a living person. Today, some fingerprint sensors can measure the frequency of dielectric current found in living human skin. Other fingerprint sensors measure the spectral response of living tissue beneath the skin through multi-spectral optical or ultrasound techniques. Techniques used with other biometric modalities like face and iris recognition can detect motion or other aspects to differentiate between a living person and a photograph. Vein recognition uses infrared light to penetrate the skin surface to measure vein patterns. Since these patterns are not visible using photographic means or other direct observations, this biometric is less vulnerable to spoofing attacks. It is also possible to combine one form of biometric measurement with another (e.g., fingerprint pattern and finger vein pattern) to reduce vulnerability to spoofing[14].

[14] "Biometric Attack Vectors and Defences," C. J. Roberts, September 2006, http://eprints.otago.ac.nz/559/1/BiometricAttackVectors.pdf