Smart Cards and Biometrics in Healthcare Identity Applications

A Smart Card Alliance Healthcare Council Publication

Publication Date: May 2012

Publication Number: HCC-12001

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 Introduction

Both smart cards and biometrics are used in identity management systems to verify individuals' identities. Biometrics alone, smart cards alone, and a combination of smart cards with biometrics are options for healthcare organizations moving to stronger, electronic identity authentication of patients and providers.

This white paper was developed by the Smart Card Alliance Healthcare Council to:

- Provide an overview of smart card and biometric technologies;
- Discuss the key considerations for selecting biometric and smart card technology for identity verification; and
- Describe the benefits of combining smart cards and biometrics for identity applications.

2 Smart Card Technology and Biometrics Technology: An Overview

2.1 What Is Smart Card Technology?

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, electronic passports, and USB-based tokens.[1]

Smart cards are used in many applications worldwide, including:

- Healthcare applications – citizen health ID cards, physician ID cards, portable medical record cards
- Secure identity applications – employee ID badges, citizen ID documents, electronic passports, driver's licenses, online authentication devices
- Payment applications – contact and contactless credit/debit cards, transit payment cards
- Telecommunications applications – GSM SIMs, pay telephone payment cards

Over 5 billion smart cards are shipped annually.[2] Smart card-based healthcare ID cards are issued in many countries; France and Germany, for example, have issued over 140 million smart healthcare ID cards to their citizens. Smart card technology is currently used in the Department of Defense Common Access Card (CAC), the Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) card (with over 5 million issued to all federal employees and subcontractors), the Transportation Worker Identification Credential (TWIC), and the U.S. electronic passport. Smart card technology is also built into every GSM mobile phone's subscriber identity module (SIM) and in the contactless credit and debit cards issued by the financial industry.

Globally, the payments industry is migrating from magnetic stripe bank cards and infrastructure to smart payment cards based on the Europay MasterCard Visa (EMV) specification. Over 1.5 billion smart card-based credit and debit cards are now issued globally and 21.9 million point-of-sale (POS) terminals accept EMV cards as of Q4 2011. Eighty countries globally are in various stages of EMV chip migration, including Canada and countries in Europe, Latin America and Asia, with migration to EMV smart payment cards now starting in the U.S.

2.2 What Are Biometric Technologies?

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.

2.2.1 Biometric System Components and Process

Four major components are usually present in a biometric system:

[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."

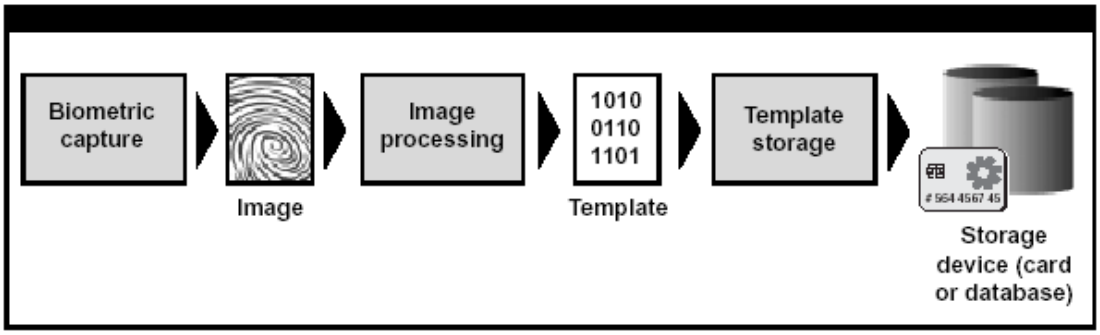
[2] Source: Eurosmart, http://www.eurosmart.com

- A mechanism to scan and capture a digital representation of a living person's biometric characteristic.
- Software to process the raw biometric 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 biometric sample.
- An interface with the application system to communicate the match result.

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

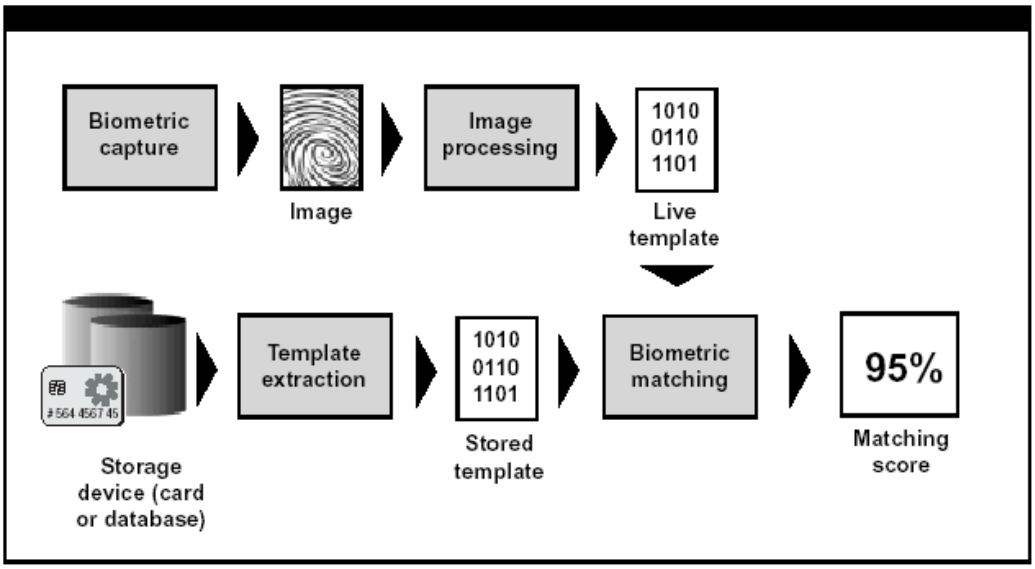
Enrollment. As shown in Figure 1, the biometric sample of the individual is captured during the enrollment process (e.g., using a sensor for fingerprint, microphone for speech recognition, camera for face recognition, camera for iris recognition). The unique features are then extracted from the biometric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

2.2.2 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[3]

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

[3] High, medium and low are denoted by H, M, and L, respectively. Values assigned for how each biometric identifier meets 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 (i.e., 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).

3 Identity Applications using Biometrics

Biometrics may be used alone or in conjunction with smart card technology in identity applications. When used alone, biometrics provide one factor of authentication – something the user is – to an identity system. For a biometrics only system, an individual would be enrolled with a biometric as described in Section 2. The enrolled biometric template would be stored on the card or in a database for later matching during the identity verification process. This section discusses the challenges of biometrics-only identity applications, compares biometrics-only implementations to smart health cards with and without biometrics and describes the advantages of combining biometrics with smart cards.

3.1 Challenges of Biometrics-Only Identity Applications

3.1.1 Central Storage of Biometrics: Impact on Security and Privacy

The key social issue surrounding biometrics is the seemingly irrevocable link between biometric traits and a persistent information record about a person. Unlike most other forms of recognition, biometric techniques are firmly tied to an individual's physical traits. The tight link between personal records and biometrics can have both positive and negative consequences for individuals and for society at large. Convenience, improved security, and fraud reduction are some of the benefits often associated with the use of biometrics.

In order to achieve these benefits for a biometrics-based authentication method, the particular biometric trait(s) must be stored remotely (centrally or distributed) in order to be available to multiple systems. Remote storage raises concerns about what security measures are in place to protect the biometric information, what personnel have access to the stored information, and how the individual's privacy and civil liberties are protected. In order for multiple systems to have access to the database for authenticating individuals' identities, both an open application interface and tightly controlled and monitored access control mechanisms are required. However, as a system becomes more widely available, there is greater risk of a system or personnel security breach. Data breaches are a significant and growing problem for the healthcare industry. The U.S. tally of major healthcare information breaches now includes 409 incidents affecting more than 19.2 million individuals since September 2009.[4]

The large-scale programs that use biometric technology to authenticate individuals are typically closed environments (i.e., performing identity authentication for a defined population and for one specific purpose) and generally use proprietary technology. The reasons for choosing a closed, biometric system are usually the business case, the time required for implementation, and the cost justification to satisfy only the current need. Closed environments are not concerned with interoperability with other organizations or programs, or with the sharing of data. Central management and control are critical to the operation of the closed environment.

These large programs are mostly government-based such as US VISIT, which collects biometric data on every individual from non-visa-waiver countries entering the the U.S., and Unique ID India, which plans to collect biometric data for 1.2 billion residents.[5] In these cases, central management of the biometric data is the responsibility of the government. Healthcare industry applications using biometric data would not use this model.

Biometric systems have the potential to collect and aggregate large amounts of information about individuals. Almost no popular discussion of biometric technologies and systems takes place without reference to privacy concerns, surveillance potential, and concerns about large databases of personal information being put to unknown uses. Privacy issues arise in a cultural context and have implications for individuals and society even apart from those that arise in legal and regulatory contexts. The problems arising from aggregating information records about individuals in various information systems

[4] "Breaches Affecting 500 or More Individuals," U.S. Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

[5] The U.S. Federal government PIV card is an exception in that it uses an interoperable biometric template to allow multi-agency applications.

and the potential for linking those records through a common identifier go well beyond biometrics, and the challenges raised have been addressed extensively elsewhere.

Although processing and sharing biometric information can bring many benefits, many concerns stem from the ease with which biometrics technology integrates with database technology, increasing the likelihood of privacy violations. For this reason, privacy must be designed into the systems from the start, rather than added on at a later time.

The protection of personal information is not the only reason for protecting biometric data. Another is the desire to prevent third parties from linking records among systems, determining the enrolled users in a system, or discovering a doppelganger (an individual who is a close match for an enrolled user). The encryption of biometric data stored in centralized databases or on a personal device such as a smart card, coupled with appropriate security measures to limit probing of the database, can be effective in countering these threats. Encryption and database protection, however, are insufficient to protect against identity theft by an attacker impersonating an individual by mimicking his or her biometric traits.

A biometric authentication method as the only identity authentication factor also offers the relying application little room for flexibility and growth.

3.1.2 Central Storage of Biometrics: System Availability

Central storage of biometric data requires systems to be online in order to validate individuals' identities. If there are system or network outages, biometric identity verification will not be available. To improve system availability, designers may then decide to store biometric information locally, which exacerbates the privacy and security concerns discussed in Section 3.1.1.

3.1.3 Availability of Biometric

The effectiveness of a biometric system can be affected by the cultural, social, and legal considerations that shape the way in which people engage and interact with these systems. Individuals' deliberate choices about whether and how to engage and their inadvertent actions both affect system performance.

For example, some individuals may choose not to place their fingers on a fingerprint scanner for fear of contracting a disease, or may be unable to do so because long fingernails are highly valued by their social group, or because an unfortunate accident occurred that removed the identifying finger or hand. Similarly, some individuals may avoid having their photographs taken for a facial recognition system because of concerns about how the images will be used; others may have concerns about the absence of customary adornments to the face (for example, scarves). In both cases, system performance may be compromised since the selected biometric may not be available for all individuals.

Additionally, collecting multiple biometric traits for authentication can be cost-prohibitive for the purpose intended. The proportionality of a biometric system—that is, its suitability, necessity, and appropriateness—in a given context will have a significant effect on users' acceptance of that system.

3.1.4 False Acceptance Rate / False Rejection Rate: Impact on System Usability

Key aspects of operational effectiveness include: recognition error rates; speed; cost of acquisition, operation, and maintenance; data security and privacy; usability; environmental conditions; and user acceptance. Generally, trade-offs must be made across all of these measures to achieve the best-performing system consistent with operational and budgetary needs. For example, recognition error rates might be improved by using a better, but more time-consuming, enrollment process; however, the time added to the enrollment process could result in queues (with loss of user acceptance) and unacceptable costs.

3.1.5 Lack of Support for other Healthcare Card Features

Healthcare organizations are not only looking to improve patient and provider identity verification, but also are seeking to streamline processes, improve quality of care and reduce costs. Biometrics-only identity applications can only support identity verification and provide no capabilities to offer other functionality

that can deliver significant benefits (e.g., multi-factor authentication for provider logon, portable emergency medical records, interoperable health record exchange with other healthcare organizations). Section 3.2.4 provides additional details on the types of functionality that can be delivered with a smart healthcare card.

3.2 Benefits of Combining Smart Cards and Biometrics

When implementing biometrics in an identity application, combining the biometrics implementation with a smart card brings a number of benefits.

3.2.1 Enhanced Privacy

Using smart card technology significantly enhances privacy in biometric ID systems. Smart cards can store and match the biometric on the card, enhancing user privacy. In this implementation, the enrolled biometric template is stored in the smart card's secure memory. When a biometric match is requested, the biometric reader 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 identification system. This method protects the initial enrolled biometric 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.

3.2.2 Enhanced Security

An ID system using the combination of smart card technology, cryptographic functions and biometrics has significant security advantages, including:

- Using digital signatures to ensure that the biometric template being used has not been altered.
- Using encryption to protect the biometric template and other personal information stored on the smart card.
- Using the smart card to compare the live biometric template with the biometric template stored on the card. Since the biometric template never leaves the card, this protects the information from being accessed during transmission and helps to address users' privacy concerns.
- Using a cryptographic challenge to authenticate the legitimacy of the card and the reader. 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.

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, offline identity verification. Local identity verification can reduce the time to authenticate an individual's identity, allowing faster verification, and eliminate the need for the identity verification to require a central system.

3.2.4 Support for other Healthcare Functions

Smart cards can also support a wide variety of functions to improve healthcare provider and insurer processes, including [6]:

- Storing all necessary applications and healthcare information on the card, enabling offline access to up-to-date critical healthcare information when a patient is receiving medical care from multiple providers and/or in an emergency situation.
- Allowing easy update of information stored on the care after issuance. Patient healthcare information can be written to and updated on the card by authorized healthcare providers, with

[6] Additional information on the use of smart cards for healthcare applications can be found on the Smart Card Alliance web site, http://www.smartcardalliance.org/pages/smart-cards-applications-healthcare-identity

updated information then available to both the patient and other healthcare providers (if authorized) to access.

- Facilitating record exchange and assisting with coordination of care among multiple healthcare providers by storing multiple patient identification or patient record identification numbers on the smart card.
- Quickly and accurately identifying patients, reducing medical identity theft and improving quality of care.
- Streamlining patient registration and patient information access at any points of care, reducing routine paperwork and eliminating errors.
- Supporting audit logging and remote access accountability.
- Enabling secure access to healthcare websites.

3.3 Comparison of Approaches

Table 1 outlines several key functionality requirements that arise in healthcare applications and how a biometric alone, a smart card alone and a combined smart card and biometric solution would address the requirement.

Table 2. Healthcare Functionality and Implementation Approaches

Key Functionality for Healthcare Identity Application	Biometric Alone	Smart Card Alone	Smart Card and Biometric Combined
Maximizes security by enabling multi-factor authentication (e.g., ID photo + PIN authentication + biometric)	No	No	Yes
Enables opportunities for branding, loyalty, incentives and reward programs	No	Yes	Yes
Can be used by everyone	No (e.g., limited by poor fingerprint ridges, children)	Yes	Yes
Has redundant features for identity authentication	No – if biometric system is unavailable, identity authentication is not possible	Yes – card typically has multiple features that can be used for identity authentication	Yes – if biometric identity authentication fails, other card features can be used
Works only when connected with a database	Yes – database may be local or remote	No – card can support local authentication process (e.g., PIN comparison on card)	No – card can support local biometric match-on-card
Provides a portable solution for authentication	Low – systems must all support biometric authentication	High	High

Key Functionality for Healthcare Identity Application	Biometric Alone	Smart Card Alone	Smart Card and Biometric Combined
Provides security for the identity data and the identity authentication process	Medium – particularly the case when biometric data is transmitted by a network to a central database	High – particularly when authentication is done on the card	High – particularly when matching is done on the card
Verifies authenticity and trustworthiness of reader terminal(s), eliminating risk of passing biometric data to an unauthorized reader	No	Yes	Yes
Has good user acceptance (familiar and accepted identity verification form factor, readily adopted)	No	Yes	To be determined – new to market
Provides a sanitary method for identity verification	Depends on biometric selected	Yes	Depends on biometric selected
Provides a non-intrusive identity verification process	No	Yes	Mixed
Enables high overall system security	High	High	Highest
Works offline	Depends on application and location of biometric	Yes	Yes

4 Summary and Conclusions

Healthcare organizations considering different approaches for verifying patient and healthcare provider identity must look at the privacy, security, usability and performance implications of the different options. Smart health ID cards – either alone or combined with biometrics – provide a privacy-sensitive, secure solution, and also offer additional features and functions that can provide significant benefits to healthcare providers when compared to a biometrics-only solution.

Biometrics-only solutions are not ideal for patient health ID cards. A smart health ID card with a photo provides a solution that patients are familiar with and will readily accept. In addition, the smart health ID card promotes the healthcare organization brand, can support a wide variety of applications that add value, and can be interoperable and usable among disparate groups.

Either a smart provider ID card or a smart provider ID card with a biometric can provide healthcare organizations with the features needed to authenticate provider identities and offer better performance than a biometrics-only solution. Providers need an identity authentication solution that can be used at multiple facilities and in emergency situations. Smart health ID cards are built on standards, can be interoperable across multiple locations, and can be used with portable readers in emergency response situations. For multi-factor authentication, a smart ID card with a personal identification number can be significantly more cost-effective for a healthcare organization than a biometric solution.

Combining smart cards and biometrics can provide a full-feature solution for healthcare provider identity authentication. By storing the biometric and performing the biometric match on the smart ID card, the privacy and security of biometric authentication are enhanced and system performance is improved, with local, offline identity authentication.

Only identity verification solutions based on smart card technology can provide identity assurance and authentication while increasing privacy and security. Smart cards also bring operational efficiencies to the healthcare system that reduce costs, reduce fraud, and increase patient satisfaction. As electronic health records (EHRs) and personal health records (PHRs) move to the mainstream, smart health ID cards can be used as a two-factor authentication mechanism into a provider or insurer web portal. Smart health ID cards protect patient privacy and security when accessing online records and support the National Strategy for Trusted Identities in Cyberspace (NSTIC),[7] which identifies consumer access to online electronic health records as warranting two-factor authentication.

Smart card technology is used globally for secure identity, access and payment applications. As a standards-based technology, smart card solutions for patient and provider identity management are deployed around the world and are available from numerous vendors. Smart card technology provides a strong foundation for health ID cards, enabling improvement in healthcare processes and in patient and provider identity verification, while securing information and protecting privacy.

.

[7] http://www.nist.gov/nstic/

5 Publication Acknowledgements

This document was developed by the Smart Card Alliance Healthcare Council to provide an overview of smart card and biometric technologies, discuss the key considerations for selecting biometric and smart card technology for identity verification, and describe the benefits of combining smart cards and biometrics for identity applications.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance thanks the Council members for their contributions. Participants involved in the development of this document included: ABnote Group; Computer Sciences Corp. (CSC); Datacard Group; Gemalto; LifeMed ID, Inc.; Oberthur Technologies; OTI America; Watchdata Technologies Pte Ltd; XTec Incorporated.

Special thanks go to **David Batchelor**, **Anna Fernezian**, **Hugh Gilenson**, **Michael Magrath** and **Cathy Medich**, who developed content for the white paper.

Healthcare Council members who participated in the development and review of the white paper included:

- **David Batchelor**, LifeMed ID, Inc.
- **Louis Bianchin**, Watchdata Technologies
- **Anna Fernezian**, CSC
- **Hugh Gilenson**, ABnote Group
- **Brent Iles**, Datacard Group
- **Michael Magrath**, Gemalto
- **Cathy Medich**, Smart Card Alliance
- **Rick Pratt**, XTec Incorporated
- **John Rego**, OTI America
- **Jim Zalnasky**, Oberthur Technologies

About the Smart Card Alliance Healthcare Council

The Smart Card Alliance Healthcare Council brings together payers, providers, and technologists to promote the adoption of smart cards in U.S. healthcare organizations. The Healthcare Council provides a forum where all stakeholders can collaborate to educate the market on how smart cards can be used and to work on issues inhibiting the industry. Healthcare Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

6 Appendix: Resources

6.1 Smart Card Alliance Healthcare Resources

- Healthcare Identity Resources. This resource page lists Smart Card Alliance reports and industry organizations, resources and news relating to healthcare identity.

6.2 Smart Card Alliance Healthcare Reports

- A Healthcare CFO's Guide to Smart Card Technology and Applications. Developed for healthcare CFOs, this white paper outlines the key benefits and business case for using smart cards for healthcare applications. The white paper identifies some of the major challenges faced by healthcare CFOs and discusses how smart card technology can provide innovative, practical and cost-effective solutions.
- Complementary Smart Card Guidance for the WEDI Health Identification Card Implementation Guide. This document serves as a supplement to the WEDI Health Identification Card Implementation Guide, provides WEDI-compliant smart card designs and discusses the features and benefits of smart ID cards for healthcare providers and payers.
- Effective Healthcare Identity Management: A Necessary First Step for Improving U.S. Healthcare Information Systems – A Smart Card Alliance Brief for Government Policy Makers and Other Stakeholders. Government policy makers are looking carefully at the best ways to improve the efficiency of information systems in the healthcare industry. Much emphasis has been placed on the need for electronic health records for every American, and at ways to exchange those records at the regional, state and national levels. But this is putting the cart before the horse. Such an effort must start with the accurate identification of each person receiving healthcare services or participating in healthcare benefit programs. Next, there must be a way to uniquely and securely authenticate that person across the healthcare system, including over the Internet, in a secure and privacy sensitive way. This brief was developed by the Smart Card Alliance Healthcare and Identity Councils to introduce the current problems with healthcare identity management, security and privacy, and propose leveraging existing federal standards and technologies already used in other government identity programs.
- Getting to Meaningful Use and Beyond: How Smart Card Technology Can Support Meaningful Use of Electronic Health Records. "Meaningful use" has the top priority of today's healthcare industry. In 2010, the government, healthcare organizations, consumers and technology providers came together to move toward interoperable electronic health records that can transform the healthcare industry. This white paper outlines the ways in which smart card-based systems can better position healthcare organizations and providers for meaningful use of electronic health records, while addressing many of the security and privacy challenges that come with electronic health records and health data exchange.
- Healthcare Identity Management: The Foundation for a Secure and Trusted National Health Information Network. Policy makers are looking carefully at the best ways to improve our healthcare system with much emphasis being placed on the need for electronic health records for every American. This effort also includes creating an infrastructure to allow the exchange of these records at the regional, state and national levels. This paper introduces the current challenges and explains why identity management in healthcare is an essential and foundational element that must be made a priority by policy makers in order to achieve the goals of widespread use of electronic health records to support the secure and seamless exchange of healthcare information. The paper also recommends best practices for introducing a healthcare identity management infrastructure–one that provides the needed security and privacy controls that should be specified by policy makers.

- HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements. This report describes how smart cards can be used to meet HIPAA Security Rule and Privacy Rule requirements.
- Identity Management in Healthcare webinar. Accurately linking patients with their personal medical information and managing patient information are significant problems today for hospitals, other healthcare providers and healthcare payers that impact administrative efficiency, revenue collection, legislative compliance and patient quality of care. This educational webinar provided a detailed review of how healthcare organizations are facing increasing regulatory challenges that will require new approaches to address patient identification and securely authenticating patient health data.
- Medical Identity Theft webinar. Medical identity theft is a serious and growing threat. This web seminar reviewed of the scope of the medical identity theft problem, the impact that electronic health records and health information exchanges have on privacy, the critical policy requirements that address medical identity theft, and the approaches being taken to protect patient health records.
- Medical Identity Theft in Healthcare. Healthcare data breaches and medical identity theft are growing problems as the healthcare industry moves to electronic health records and health information exchanges. This brief describes the security and privacy issues that the healthcare industry is facing and advocates that the industry move to strong identity management practices and technology solutions to improve the privacy and security of health information systems and electronic health records.
- Protecting Your Health Information: Raising Public Awareness of the Privacy and Security Challenges of Healthcare Information Management. The Smart Card Alliance and Secure ID Coalition held a briefing at the National Press Club to discuss security and privacy concerns with health information. The briefing featured a panel of experts who discussed how healthcare information privacy, identity management, access and authentication are critical elements in getting the nation's healthcare infrastructure right. Video from the event is available.
- Smart Card Alliance Healthcare Council
- Smart Card Applications in the U.S. Healthcare Industry. This report describes the value that smart cards deliver in a variety of U.S. healthcare applications. The report reviews key challenges that the U.S. healthcare provider industry faces and examines the key drivers for implementing smart card-based systems to address these challenges.
- Smart Card Technology in Healthcare: Frequently Asked Questions. Smart cards are used worldwide to improve security and privacy of payment and identity applications. The Smart Card Alliance Healthcare Council developed this document to answer questions about how smart cards work and how the technology is used to manage patient identity and protect a healthcare consumer's personal information.
- Smart Cards in U.S. Healthcare: Benefits for Patients, Providers and Payers. This white paper describes the challenges within the healthcare industry and the clear opportunities for the use of smart card technology for security and privacy in healthcare. The paper examines smart card use in healthcare today and suggests additional applications for consideration.
- Smart Health ID Cards: Addressing Challenges with Patient Identity Management and Authentication Webinar. Accurately identifying and authenticating patients are significant problems for hospitals, other healthcare providers and healthcare payers that impact administrative efficiency, revenue collection, legislative compliance and patient quality of care. This webinar focused on smart health ID cards for patients, reviewing the key challenges with patient identity management and authentication today and discussing how patient ID cards and smart card technology can address the critical issues. The American Medical Association Health Security Card pilot and the Wyckoff Heights Medical Center medical smart cards were featured as examples of smart health ID card programs.