Smart Card
Alliance

Smart Card Technology and the National Strategy for Trusted Identities in Cyberspace (NSTIC)

A Smart Card Alliance Identity Council White Paper

Publication Date: June 2013

Publication Number: IC-13002

\

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.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

TABLE OF CONTENTS

1 Introduction

Internet use is evidently the most indispensable activity of our generation. We use it for almost everything—to connect with friends, shop, bank, blog thoughts, and seek medical attention, among other things. But as use of the Internet has increased, so has cyber crime. Cyber crime has resulted in losses to individuals and businesses amounting to billions of dollars annually.

According to the Federal Bureau of Investigation, identity theft is currently the leading and most persistent financial crime. Approximately 12 million Americans have been affected by identity theft of some kind in the past 2 years. To use their online accounts, people must remember an unmanageable number of passwords. For this reason, most people reuse the same passwords for years, making it easy for identity thieves and hackers to do their worst. To use the Internet safely and effectively, a better way must be developed for individuals to prove online that they are who they say they are.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a White House initiative to improve on the credentials currently used to access the Internet and authenticate identity online. This initiative proposes a marketplace that allows people to choose among multiple identity providers, both private and public, who can issue trusted credentials.[1] NSTIC has already involved itself in defining the essential fundamental elements that aid in strengthening identity, privacy, and security in the administration of Social Security benefits, immigration, healthcare, and other programs in the physical world. The NSTIC framework recognizes grave inadequacies in the current management of identity, privacy, and security in online transactions.

The Smart Card Alliance, a non-profit industry association that includes both technology providers and financial, enterprise, and government users, is promoting the adoption of the NSTIC framework. The Alliance strongly agrees with the use of federal, state, and local government initiatives to accelerate the development of an identity ecosystem. At the same time, the Alliance advocates for leveraging existing procedures, standards, and technology. Technologies such as those described in *FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors* and in the *Federal Identity, Credentialing and Access Management Roadmap* are vital to achieving interoperable, high assurance identity verification.

Smart card technology provides maximum security through strong authentication mechanisms and protects user privacy. The technology is designed to resist malware, forgery, and other efforts to extract information fraudulently from an identity token. Smart card technology provides a tamper-proof container for digital identity credentials and biographic and biometric identifiers. The availability of multiple form factors make smart card technology-based tokens portable and easy to distribute.

This white paper reviews the NSTIC initiatives and discusses how smart card technology can provide the advanced credentialing capabilities needed to enable high assurance in the NSTIC identity ecosystem.

[1] National Strategy for Trusted Identities in Cyberspace, “Enhancing Online Choice, Efficiency, Security and Privacy,” The White House, April 2011.

2 NSTIC Overview

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a White House initiative to collaborate with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions.[2]

2.1 Purpose of the Organization

NSTIC was created in response to an action item in the *Cyberspace Policy Review*[3] that calls for the creation of an online environment in which individuals and organizations can execute transactions with confidence, trusting the identities not only of all parties to the transaction but also of the infrastructure supporting the transaction. This environment of trusted identities and infrastructure is referred to as the *identity ecosystem*. The identity ecosystem is an online environment in which individuals and organizations can trust each other, because they agree to follow specific standards to obtain and authenticate both their digital identities and the digital identities of all devices involved in a transaction. The identity ecosystem is designed to secure a complete range of transactions, from anonymous to fully authenticated and from low value to high value.[4]

By enabling the principles of NSTIC, individuals no longer have to remember an ever-growing (and potentially insecure) list of user names and passwords to access various online services. NSTIC envisions an environment where individuals use a secure, interoperable, privacy-enhancing credential to authenticate themselves online for different types of transactions. The credential can be any number of identity tools and can be stored on a variety of different identity tokens (such as a smart card or a USB device). The credential comes from a public or private provider. The security level and abilities of the credential can vary, depending on the provider and medium.

2.2 Credential Definition

NSTIC envisions an entity known as an *identity provider* (IDP), which is responsible for establishing, maintaining, and securing the digital identity associated with a particular person. The IDP’s responsibilities include revoking, suspending, and restoring the person’s digital identity if necessary. IDPs issue *credentials*: information objects that provide evidence of the person’s identity for a transaction. The credential may also provide a link to a person’s authority, roles, rights, privileges, and other attributes.[5]

According to NIST Special Publication 800-63 *Electronic Authentication Guideline*, a credential is an object that authoritatively binds a person’s identity to a token possessed and controlled by that person. A securely issued smart card or smart card technology-based device can carry a credential and provide the owner with many benefits for safeguarding information.

Establishing a smart card-based identity token for an individual involves several components. First, an individual enrolls for a credential, a process which consists of identity proofing, the

[2] "About NSTIC,” http://www.nist.gov/nstic/about-nstic.html.

[3] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, The White House, May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[4] National Strategy for Trusted Identities in Cyberspace, *Enhancing Online Choice, Efficiency, Security and Privacy*, The White House, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[5] National Strategy for Trusted Identities in Cyberspace, *Enhancing Online Choice, Efficiency, Security and Privacy*, The White House, April 2011.

establishment of a personal identification number (PIN), and possibly the capture of biographic and biometric data. Then, the credential is produced and issued to the individual. Usually the credential must be maintained over a lifecycle, which can include revocation, reissuance and replacement, re-enrollment, expiration, PIN reset, suspension, and reinstatement processes.

Smart card technology is an important element in identity management systems, due to its ability to support authentication mechanisms that can identify people with minimal ambiguity. A smart card-based identity token can be used to verify who an individual claims to be, using information about the cardholder printed or stored on the card and biometric information stored in the card, instead of or possibly in addition to checking something the cardholder knows (such as a PIN).

Use of smart card technology within the identity ecosystem offers several advantages:

- The technology is designed to eliminate fraud by minimizing the risk that credentials or tokens are fraudulent.
- Smart cards are deployed around the world for financial services, mobile communications, healthcare, and e-government.
- Smart card technology enables secure identity verification while protecting personal privacy.
- Only the cardholder is able to initiate or verify a transaction using a PIN, biometric data, or both.
- Smart card technology-based tokens can store electronic credentials and prevent the credentials from being copied, altered, or hacked.
- Smart card technology-based tokens can hold many different identity credentials and support multiple authentication mechanisms.

As shown in Figure 1, use of smart card technology increases the security of the identity system and improves the accuracy, speed, and control of the cardholder authentication process.

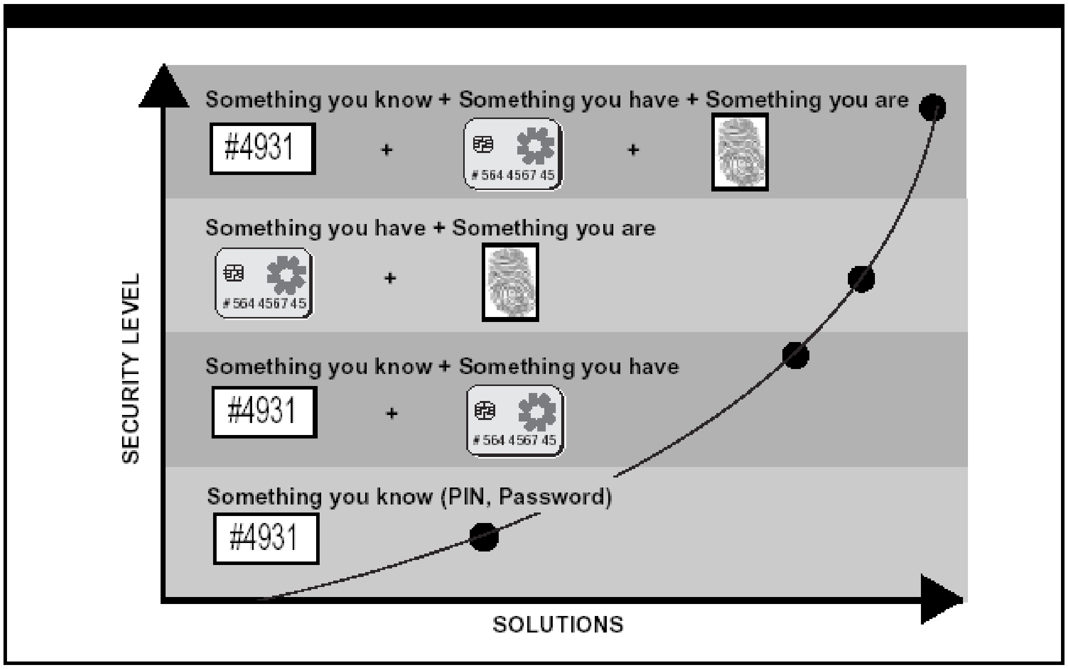
Something you know + Something you have + Something you are
#4931
+
# 564 4567 45
+
Something you have + Something you are
# 564 4567 45
+
Something you know + Something you have
#4931
+
# 564 4567 45
Something you know (PIN, Password)
#4931
SECURITY LEVEL
SOLUTIONS

Figure 1: Impact of Smart Cards on Security

2.3 Guiding Principles and Relevance to Smart Card Technology

NSTIC envisions individuals and organizations using secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.

NSTIC has identified several guiding principles[6] for the identity ecosystem. Smart card technology offers advantages in all of the areas represented by these principles (Table 1).

Table 1: NSTIC Guiding Principles and Smart Card Technology Advantages

Guiding Principal	Smart Card Technology Advantage
Identity solutions will be privacy-enhancing and voluntary	Preserves the positive privacy benefits associated with offline identity-related transactions. Provides individuals using smart cards with the freedom to present the stored credential of their choice.
Identity solutions will be secure and resilient	Is based on proven technology and security standards, so provides secure and reliable methods of electronic authentication. Can detect when trust has been betrayed, is capable of timely restoration after any disruption, can quickly revoke and recover compromised digital identity credentials, and can adapt to the dynamic nature of current technology.
Identity solutions will be interoperable	Is governed by standards for physical properties, communication characteristics, and definition of the stored applications and data. Available standards provide both technical and policy-level interoperability (e.g., ISO/IEC 7816, ISO/IEC 15693, ISO/IEC 14443, ISO/IEC 7501, ICAO, FIPS 140 (1-3), FIPS 201, EMV, PC/SC Specification, CEN and ETSI, HIPAA, IC Communications Standards, GSM, OpenCard Framework, GlobalPlatform, Common Criteria, and national and international biometric standards).
Identity solutions will be cost-effective and easy to use	Enables individuals to have many identity credentials from an array of service providers. As an identity solution, is simple to understand, intuitive, easy to use, and requires minimal user training.

[6] From http://www.idecosystem.org/page/adherence-nstic-guiding-principles

3 Authentication Levels

In recent years, Federal agencies have expanded their use of online services for conducting business transactions. For these services to be secure and protect privacy, an agency must verify the identity of users accessing the agency's system and ensure that proper authentication takes place. Office of Management and Budget Memorandum 04-04 (M-04-04)[7] provides Federal agencies with guidance to help them accomplish these goals. M-04-04 outlines a five-step process for meeting e-authentication assurance requirements:

1. Conduct a risk assessment of the agency's information system.
2. Map identified risks to a required assurance level.
3. Select appropriate technology using NIST e-authentication technical guidance.
4. Validate that the implemented information system achieves the required assurance level.
5. Periodically reassess the information system to determine technology refresh requirements.

This section describes the authentication levels that are required by Federal systems. Commercial vendors may want to achieve the same authentication levels, since the Federal standard assures a robust segmentation of transaction types.

3.1 Level of Assurance

M-04-04 describes identity authentication assurance as a degree of confidence in three areas:

- The identity proofing process used to confirm the identity of the individual who is to be issued a credential
- The credential itself
- The individual using the credential is actually the individual to whom the credential was issued

M-04-04 establishes four levels of assurance for e-government transactions; the result of the agency risk assessment will map to one of these assurance levels. The required assurance level increases as the risk and consequences of an authentication error become more serious. The four assurance levels are the following:

- Level 1: Little or no confidence that the asserted identity is valid
- Level 2: Some confidence that the asserted identity is valid
- Level 3: High confidence that the asserted identity is valid.
- Level 4: Very high confidence that the asserted identity is valid

The level of assurance is determined by analyzing the potential and likelihood of harm or impact from an authentication error. The categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information

[7] Office of Management and Budget, Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003.

- Personal safety
- Civil or criminal violation

The required assurance level for an electronic transaction is determined by assessing the potential impact of the harm caused by an authentication error (as described by each of the above categories) and evaluating whether the impact will be low, medium, or high. These impact levels are then compared to the impact profile shown in Table 2 and assigned the appropriate assurance level. The highest assurance level assigned to any impact becomes the required assurance level for the transaction. For example, if all impact levels are low, the level of assurance for the transaction is 3, because low impact on personal safety requires level 3 assurance.

Table 2. Assurance Level Assignments by Harm and Impact Level

Harm/Impact	Assurance Level Impact Profile			
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod High
Civil or criminal violation	N/A	Low	Mod	High
Assigned assurance level	**1**	**2**	**3**	**4**

3.2 Technical Requirements for Levels of Assurance

An agency must implement e-authentication at the level identified by the process described in M-04-04. NIST SP 800-63[8] provides guidelines for selecting technology that can implement the required assurance level. Specifically, SP 800-63 describes technical requirements for implementing the four levels of assurance in each of the following areas:

- Identity proofing and registration of applicants
- Selection of the token (typically a cryptographic key or password) used for authentication
- Token and credential management mechanisms used to establish and maintain token and credential information
- Protocols used to support the authentication mechanism between the claimant and the verifier
- Assertion mechanisms used to communicate the results of remote authentication if these results are sent to other parties

SP 800-63 details the requirements for each element. Table 3 summarizes the identity proofing and token requirements for each assurance level described in M-04-04.

[8] National Institute of Standards and Technology, *Electronic Authentication Guideline*, NIST SP 800-63, December 2011.

Table 3: Requirements for Identity Proofing Authentication Token

Level	Assurance Description	Required Identity Proofing	Required Authentication Token
1	Little or no confidence in the asserted identity's validity	No requirement	At least one secret-based token. Low entropy authenticators (e.g., password) require a throttling mechanism.
2	Some confidence in the asserted identity's validity	Presentation of identifying materials or information	Higher entropy token (e.g., user name and strong password).
3	High confidence in the asserted identity's validity	Verification of identifying materials and information	Multi-factor authentication (e.g., two of the following: user name and strong password, token, biometric).
4	Very high confidence in the asserted identity's validity	In-person identity proofing	Hardware token based on approved cryptography. FIPS 140-2 Level 2 certification with Level 3 physical security.

3.3 Trust Framework Solutions Initiative

NSTIC envisions an environment that allows a user to choose a credential service provider (CSP) from multiple candidate CSPs. The goal is to make online transactions safer and faster while protecting privacy. The use of online credential services and the reuse of credentials decrease the burden on users and reduce the costs for agencies. However, it increases the burden on agencies to identify and authenticate users. Accomplishing the goals of NSTIC requires the establishment of trust relationships between government agencies and third-party credential providers.

The Trust Framework Solutions (TFS) Initiative establishes the trust required to externalize authentication and leverage approved CSPs in accordance with NSTIC. A governing body called the Trust Framework Evaluation Team (TFET) uses a process called the trust framework provider adoption process (TFPAP)[9] to evaluate and approve industry-based trust frameworks.[10] The TFET receives applications and ultimately approves the adoption of a trust framework provider (TFP). TFPs in turn define the processes for evaluating whether a CSP's credentialing processes fulfill Federal requirements for issuance, privacy, and auditing as codified by OMB, NIST, and the General Services Administration (GSA). Credentials issued by a TFP-approved[11] CSP can be trusted to meet the SP 800-63 technical requirements at the level of assurance defined by M-04-04.

Use of a CSP approved under the TFS Initiative ensures the following:

- Trust, particularly trust that the CSP has implemented the appropriate processes for identity proofing and credential lifecycle management

[9] Identity, Credential, and Access Management, *Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3*, Version 1.0.1, September 4, 2009.

[10] Identity, Credential, and Access Management, *ICAM Trust Framework Providers* provides a current list of approved TFPs.

[11] Identity, Credential, and Access Management, *ICAM Trust Framework IdPs* provides a current list of approved CSPs.

- Robust and reliable technical interoperability between endpoints through the use of Federal Identity, Credential, and Access Management (FICAM) profiles[12]
- The expected level of assurance
- The required level of privacy protection

Figure 2 illustrates the TFS Initiative process.

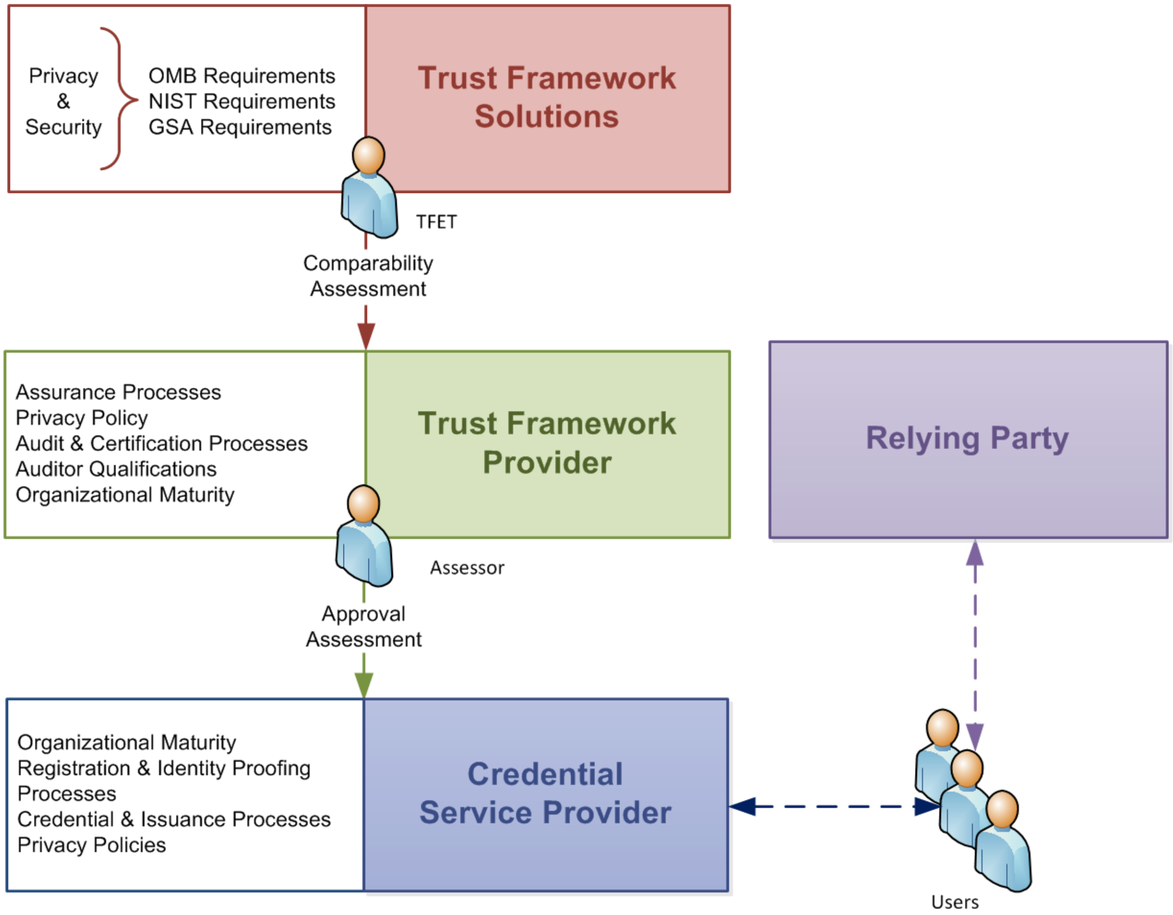

Figure 2: Trust Framework Solutions Initiative Process Overview

[12] *http://www.idmanagement.gov/programs*.

4 Smart Card Technology

Smart card technology embeds a smart computer chip in a card or other form factor. The embedded chip can carry a microcontroller, crypto-coprocessor, memory, operating system, and application software. The chip provides the smart device with built-in tamper resistance and the capabilities of storing large amounts of data securely, carrying out computing functions, and interacting intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in multiple form factors: a plastic card (with contact or contactless communication capabilities, or both, and optionally a display and keypad), a USB device, or a secure element (SE) that can be embedded in a mobile (or other) device (e.g., Subscriber Identity Modules (SIMs) or smart microSD cards).

Smart cards communicate with a reader either through direct physical contact or through a contactless interface. A typical contact smart card comprises a plastic card, an embedded chip, and a contact plate (which is visible on the surface of the card). Transmission of commands, data, and card status takes place over the physical contact points. A contactless smart card or device requires only close proximity to a reader. Both the reader and the device have antennae; they communicate using radio frequency (RF) over this contactless link.

Smart card technology can also be built into USB-based tokens, providing a portable authentication device that can be used with any computer with a USB port. These tokens can be used for any logical access applications for which a smart card can be used: secure data, password and PKI credential storage, encryption/decryption, and multifactor access to computers and networks. Smart card USB-based tokens can be designed to incorporate a chip in the SIM form factor to provide field serviceability.

With multiple standards-based form factors available, all offering the same platform capabilities, organizations can use smart card technology in the form factor most appropriate for their constituency.

4.1 Smart Card Technology and Strong Authentication

Smart card technology is typically used to enable multifactor authentication, incorporating something you have (the token) and something you know (typically a PIN that activates the smart token's cryptographic functions). Taking control of a person's digital identity requires both stealing the smart token and guessing the PIN. Cardholders know very quickly when a physical token is stolen and can contact an authority to report the stolen credentials. In addition, too many incorrect PIN guesses can lock the token. Smart card technology also supports the addition of biometrics (something you are), enabling three-factor authentication.

A single smart device can contain multiple identity credentials and applications and be used with different types of authentication mechanisms at various e-authentication levels. For example, smart card technology can support:

- Secure password file storage
- Generation of asymmetric key pairs and secure storage of PKI certificates
- Secure symmetric key storage
- Secure one-time-password (OTP) seed storage
- Secure PIN and/or biometric template storage and the ability to match the PIN or biometric factor on the smart card or device

By supporting multifactor authentication and enabling multiple types of authentication mechanisms, smart card technology can enable not only high levels of assurance, but also provide a straightforward, secure, and privacy-protective platform for implementing authentication mechanisms for all levels of assurance. By basing authentication on standardized technology and using standards-based authentication mechanisms, organizations can implement identity authentication processes that are highly compatible and interoperable.

Section 8, Appendix A, includes details on how smart card technology can be used to add value to different authentication mechanisms.

4.2 Smart Card Technology and Privacy

Identity tokens that use smart card technology have strong security features that can enhance privacy protection in a well-designed and properly implemented identity authentication system. Implemented properly, smart card technology strengthens the ability of an organization to protect the privacy of individuals whose identity the organization needs to verify. Unlike other identity tokens, smart card-based identity tokens can implement a personal firewall, releasing only required information and only when it is genuinely required.

Relying on smart card technology provides the following advantages:

- Robust information protection
- Strong ID security
- Sophisticated on-card processing
- Authenticated and authorized information access

4.2.1 Robust Information Protection

Smart card technology protects the identity data stored on the identity token completely and constantly. Smart card-based identity tokens can encrypt the identity information stored on them and encrypt communications between the identity token and the device that reads the token, preventing eavesdropping. Smart card technology can lock the personal information on the identity token, releasing it only after the owner authorizes the release by providing unique information such as a PIN, password, or biometric.

4.2.2 Strong ID Security

Identity tokens incorporating smart card technology are extremely difficult to duplicate or forge. In addition to visual anti-counterfeiting and tamper-resistance features such as holograms, microprinting, and optical variable devices that are used on the card form factor, smart card chips have built-in tamper-resistance. The chip in a smart card-based identity token includes a variety of hardware and software capabilities that immediately detect and react to tampering attempts, countering possible attacks.

4.2.3 Sophisticated On-Card Processing

Smart devices accomplish many identity management functions within the secure processing environment of the chip. Smart card technology-based identity tokens store data, which they can then manage securely, protecting the information both while it is stored and while it is being accessed. On-chip processing enables smart card-based identity tokens to perform on-card functions (for example, encryption, decryption, and other data processing) and to interact securely and intelligently with a reader.

These capabilities are particularly important when a system relies on biometric information to verify the identity of an individual. Smart card technology-based identity tokens can securely store biometric information and compare a captured biometric with the stored biometric to verify an individual's identity. This capability increases privacy: the individual's stored biometric information never leaves the token (which remains in the individual's possession) and the stored biometric is compared to the captured biometric within the smart card chip's secure processing environment.

4.2.4 Authenticated and Authorized Information Access

Smart cards and devices have the unique ability to select the appropriate action depending on their current environment. A smart card-based identity token can verify the authenticity of a reader and prove its own authenticity to a reader. Smart cards and devices can also verify the authority of an information requestor and grant access only to the information required by that particular request. Stored personal information can be protected further by a unique PIN or biometric that the individual must provide before access to the information is granted.

5 Uses of Smart Card Technology within the Identity Ecosystem

The identity ecosystem calls for various levels of assurance and must be secure and resilient (Table 1). Security and resiliency become increasingly important as the assurance level goes up; an essential element of a resilient credential is the ability to be revoked or suspended easily. Credentials at lower assurance levels can be propagated easily: relying parties can simply reference an earlier validation that is cached within their relying systems. Credentials at higher assurance levels (an excellent example is public key infrastructure, or PKI, certificates) offer much tighter controls in terms of validation processes, and relying parties own the responsibility to authenticate these credentials properly.

5.1 Required Assurance Levels

To enable high assurance transactions, institutions and individuals alike require credentials that can perform certain essential functions:

- Mutual authentication with a relying party
- Information authentication using digital signature technologies
- Non-repudiation of transactions
- Maintenance of confidentiality of transactional data.

To support these functions, both PKI and multifactor authentication are essential. The most common carrier for multifactor PKI credentials is a smart card or device. Smart card-based tokens can carry a credential that utilizes PKI certificates to enable strong digital trust and that delivers the assurance levels required for the most critical transactions within the identity ecosystem.

Biometric technologies have also emerged as strong identity verification technologies, supporting the “who you are” factor of multifactor authentication. But the biometric information must be protected, as it is highly susceptible to attack. Biometric templates need protection against substitution and may require authentication. When digitally signed and stored in smart cards and devices, biometric templates become very reliable identification factors. They can be highly resistant to tampering, and have strong non-repudiation attributes.

Smart card-based credentials can satisfy not only the identity ecosystem’s requirement for a high assurance level credential, but also the requirement for a range of identity ecosystem credentials, providing various levels of assurance to map to various levels of risk. Not all identity ecosystem transactions require high levels of security. Certain interactions may require multiple levels: transaction initiation may demand only a low level of security, which can be satisfied with a user name and password, but security may have to be “stepped-up” for subsequent transactions. For example, a customer at a financial institution may connect to a Web site to browse account status but then decide to submit a funds transfer request. The funds transfer request will require additional authentication at an assurance level higher than that used to log on to the Web site. Smart card technology-based tokens can be a repository for a variety of credential types and support a number of security protocols and authentication mechanisms.

5.2 Trust Framework Requirements

High assurance credentials must be issued within an acceptable trust framework and typically are certified with a trustmark. The trustmark attests to the relying party’s adherence to the rules of the identity ecosystem and validates the identity provider’s adherence to the framework appropriate to the transaction being performed. The policy foundation for the identity ecosystem calls for an accreditation authority to assess and validate identity providers, attribute providers, relying parties, and identity media, ensuring that they all adhere to an agreed-upon trust framework. Accreditation authorities can issue trustmarks to participants they validate.

The NSTIC identity ecosystem framework provides a set of standards and policies that apply across different frameworks. The standards include both technical and functional standards and enable specific communities of interest to agree on how to trust transactions within their own communities or across communities.

Smart card technology-based credentials have an advantage in this area, as they are already in use today. Examples include ePassports, the Department of Defense (DoD) Common Access Card (CAC) and Federal PIV card, EMV credit and debit cards, and numerous national health and national ID cards in use around the world.

5.3 Smart Card Technology Use Cases

With over 7 billion smart cards shipped annually,[13] smart card technology is used in many identity, payment, and communications applications worldwide:

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

The following sections describe several examples of such uses.

5.3.1 Payment Applications: Online Banking

Increases in counterfeit card fraud have led the financial industry to move to smart chip technology for bank cards and to develop the global EMV specifications[14] for both bank cards based on chip card technology and the accompanying point-of-sale (POS) infrastructure. Financial institutions in the United States, Europe, Latin America, Asia/Pacific, and Canada are issuing contact or dual-interface EMV smart cards for credit and debit payment or are migrating to EMV. According to EMVCo,[15] approximately 1.5 billion EMV cards have been issued globally, and 21.9 million POS terminals accept EMV cards as of the second quarter of 2012.

In the United Kingdom, the cryptographic capabilities of EMV-compliant smart bank cards have been harnessed to provide greater protection for customers undertaking online banking transactions through the use of MasterCard's Chip Authentication Program (CAP) and Visa's dynamic passcode authentication (DPA).

A transaction using CAP/DPA works as follows:

1. The cardholder is prompted to insert the EMV bank card into an offline reader.

[13] Eurosmart, http://www.eurosmart.com/.

[14] The original founders of the EMV standards body were Europay, MasterCard, and Visa—hence the acronym EMV. Information on the specifications is available at http://www.emvco.com.

[15] EMVCo is the organization formed in February 1999 by Europay International, MasterCard International, and Visa International to manage, maintain, and enhance the EMV Integrated Circuit Card Specifications for Payment Systems. EMVCo is currently operated by American Express, JCB International, MasterCard Worldwide, and Visa, Inc.

2. The reader prompts the cardholder to enter a PIN, which is checked by the card.
3. For every use, the bank can issue a challenge.

   The challenge is a number of up to 8 digits, which the bank determines dynamically.
4. The cardholder types the challenge into the reader, which transmits it to the card.

   If the card has previously verified the PIN, it generates a passcode that is an encrypted version of the challenge and of additional information that identifies the card and ensures that every passcode is different (and thus cannot be replayed, even if the challenge happens to be the same).
5. The cardholder types in the passcode for transmission to the bank.
6. The bank verifies that the passcode could only have originated from the card associated with the account, that the card has been given the correct PIN and challenge, and that the passcode has been produced in the correct sequence for that card.

This process offers greatly enhanced levels of security for online banking transactions and has been implemented by many of the major UK banks. The use of end-to-end application level cryptography (based on keys shared between the card and the issuer) provides strong authentication and defeats attacks such as the man-in-the-middle (MitM) attack. Such protection represents a significant improvement over user name and password protection, which is very vulnerable to variations on the MitM attack, such as the man-in-the-browser (MitB) attack. Even accounts protected using OTPs can be more vulnerable to these attacks than those protected by more comprehensive strong cryptographic mechanisms.

An essential feature of the CAP/DPA solution is its ability to support transaction-level authentication (signing), which protects against attacks such as MitB. Moreover, the CAP/DPA solution achieves the goal of enhanced security while maintaining processes that are simple, convenient, and easily adopted by banking customers.

5.3.2 Identity Applications: Government-Issued Credentials

Government use of smart card technology is increasing worldwide, including issuance of citizen identity credentials, government employee identity credentials, social benefits credentials and healthcare credentials.

Electronic passports based on contactless smart card technology have become the norm. A strong international standard and effective trust framework enable these credentials to be accepted around the world. In some countries, the ePassport includes biometrics.

In particular, the U.S. Federal Government has adopted smart card technology for major credentialing initiatives. The DoD CAC uses smart card technology to credential all military and civilian personnel. CACs are the standard DoD ID card and the primary card enabling both physical access to buildings and logical access to DoD computer networks and systems.

In compliance with Homeland Security Presidential Directive 12, all Federal employees and contractors now receive a smart card-based identity credential: the PIV card, defined by FIPS 201.[16] While only Federal agencies can issue the PIV card, enterprises can follow FIPS 201 processes, use FIPS 201 defined technologies, and implement credentials that are PIV interoperable or PIV compatible, as appropriate.[17] Following the FIPS 201 process for credential

[16] National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

[17] *Personal Identity Verification Interoperability for Non- Federal Issuers*, http://www.idmanagement.gov/documents/personal-identity-verification-piv-interoperability-non-federal-issuers

issuance allows all Federal relying parties to trust the card across enterprises. This trust is established by common enrollment, registration, and issuance processes and by the use of a strong authentication credential that leverages a cross-certified and federated public key infrastructure.

Other Federal Government ID programs have also started to use smart cards, including the Transportation Worker Identification Credential (TWIC) and the First Responder Authentication Credential (FRAC). Under the Transportation Security Administration TWIC program, biometric-enabled identity smart cards are issued to all private and commercial transportation workers accessing U.S. maritime ports.

5.3.3 Healthcare Applications: Healthcare Information

Healthcare organizations can benefit by using smart card technology to provide authenticated access to medical information and identities. Smart cards can be used to implement strong identity authentication and information security for healthcare organizations and applications.[18] Smart healthcare cards protect patient privacy and security when accessing online records and support the National Strategy for Trusted Identities in Cyberspace (NSTIC), which identifies consumer access to online electronic health records as warranting two-factor authentication.

5.3.3.1 Compliance with the Health Insurance Portability and Accountability Act

Healthcare organizations are required by the Health Insurance Portability and Accountability Act (HIPAA) to safeguard patient health information. HIPAA specifies administrative, technical, and physical security procedures to assure the confidentiality of protected health information. The security of confidential health information is essential to HIPAA compliance and patient privacy. Secure access management fulfills the Act’s patient privacy requirements. The combination of smart card-provided cryptography, authentication, system security, and policy can implement strong authentication within an organization’s healthcare systems. The smart card can be used for administrative, data, network, and physical security.

5.3.3.2 Portable Medical Records

Numerous pilots and applications have demonstrated the use of smart cards to implement portable medical records and secure and control access to distributed repositories of patient health records and insurance data, such as detailed medical histories, medical images, x-rays, and insurance information.

A smart healthcare card can authenticate a patient’s identity and facilitate rapid access to medical information about that patient. A smart card solution that stores (or points to stored) health information, conditions, prescriptions, and insurance data can result in better service and shorter medical visits. The card can also be used to help parents provide and update immunization records for school-age children.

5.3.3.3 Medical Identity Theft Mitigation

Identity theft and fraud continue to be significant problems in social, workplace, business, and medical interactions. Strong electronic authentication of patients, insurance personnel, and healthcare personnel can help providers mitigate the risks posed by identity theft. Authentication can include every person receiving care and every person who accesses patient information.

[18] Additional information on the use of smart card technology for healthcare applications can be found on the Smart Card Alliance Healthcare Identity Resources Web page, http://www.smartcardalliance.org/pages/smart-cards-applications-healthcare-identity.

A multifactor authentication solution that identifies the patient, the medical provider, and all others handling patient information can span data locations while maintaining privacy and facilitating the secure exchange of medical information.

5.3.3.4 Emergency Medical Information

Emergency personnel and first responders need medical information for a patient immediately. Using smart cards and portable readers, emergency information can be available at any location: the site of an emergency, during patient transfer, or within a healthcare facility's emergency room, enabling first responders to manage and coordinate life-saving information.

A smart healthcare card can store a patient's identity and medical records, providing medical personnel with critical information even when the patient is unconscious or too flustered to convey information, or when there is a language barrier. Health information such as special medical conditions, prescriptions, and insurance eligibility data can be stored on the card, and emergency solutions can be implemented that both access on-card information and point securely to online medical data repositories.

5.3.3.5 Healthcare Provider Identification Credential

As healthcare providers migrate their records from paper to electronic media, there is growing industry awareness of the need for secure and encrypted data solutions. The lack of provider identity verification can compromise patient privacy if unauthorized users access patient records and can cause health risks for patients if records are compromised or manipulated.

Use of a smart healthcare card can allow organizations to implement strict security access controls for health information. The use of large clinical data exchanges makes it critical for user privileges to be assigned using role-based access controls and implement multifactor authentication. Smart cards can identify and authenticate an individual who requests access to medical information systems.

Smart card identity credentials are currently being deployed in hospitals and healthcare organizations as secure employee identity credentials. The credentials allow healthcare providers to control physical access to assigned areas, permitting only authorized personnel to enter. Controlled areas can include the pharmacy, operating room, network server room, or HR department. The same credential can also be used to authorize logical access to networks and computers and support HIPAA compliance. Implementing multifactor authentication and the cryptography capabilities supported by smart cards can provide benefits in the form of stronger identity verification and can help ensure corporate network security.

In addition, the PIV-I credential has been recommended by FEMA in the "National Incident Management System (NIMS) Guideline for the Credentialing of Personnel" (July 2011) and is the credential being deployed as the First Responder Authentication Credential (FRAC) by several state and local governments. The PIV-I credential is standards-based, non-proprietary, trusted by the federal government, and usable for multiple purposes. The first responder population encompasses approximately 20 million people in the U.S.; healthcare professionals represent a significant percentage of this population including the nation's one million physicians and three million nurses and EMTs. By putting a FRAC in the hands of the medical community, local authorities will be able to rapidly grant access only to qualified individuals during emergency situations, such as Hurricane Katrina and Hurricane Sandy. If followed, the PIV-I guidance provides a supporting framework for technical interoperability with the nearly 10 million federally-credentialed uniformed and civilian employees and contractors. It supports enhanced integration and reduced costs in day-to-day operations as well as during response and incident management.

6 Conclusions

The National Strategy for Trusted Identities in Cyberspace (NSTIC) was released in April 2011, with the main objective of encouraging the private sector, in collaboration with Federal colleagues, to develop online identity and authentication systems that individuals could use and that organizations and commercial stakeholders could all accept without each needing to create their own vetting systems.

The flexibility of smart card technology makes it a valuable component of the NSTIC landscape, supporting multiple prerequisites:

- Management of a participant's multiple online identities
- Participant control of presentation
- Preservation of anonymity
- Robust security
- Interoperability among participants

Smart card technology can meet the challenges presented by a heterogeneous identity framework while providing assurance that transactions are secure. While the details of the NSTIC identity ecosystem are still being defined, smart card technology provides a secure flexible solution and is the best choice for higher assurance levels.

7 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Identity Council to describe the benefits of combining smart card technology and strong credentials within the National Strategy for Trusted Identities in Cyberspace (NSTIC).

Publication of this document by the Smart Card Alliance does not imply endorsement by 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 included: Booz Allen Hamilton; CH2M HILL; Deloitte & Touche LLP; Gemalto; General Services Administration (GSA); HP Enterprise Services; IDmachines; IQ Devices; NXP Semiconductors; Oberthur Technologies; SecureKey Technologies.

The Smart Card Alliance thanks **Abel Sussman**, Booz Allen Hamilton, who led this project and the following individuals who contributed content or participated in the development and review of this document:

- **Rene Bastien**, SecureKey Technologies
- **Stu Cox**, Oberthur Technologies
- **John Esser**, Oberthur Technologies
- **Frazier Evans**, Booz Allen Hamilton
- **Sal D'Agostino**, IDmachines
- **Chris Gardner**, SecureKey Technologies
- **Bryan Ichikawa**, Deloitte & Touche
- **Judy Keator**, HP Enterprise Services
- **Cathy Medich**, Smart Card Alliance
- **Neville Pattinson**, Gemalto
- **Raj Pillai**, GSA
- **Steve Rogers**, IQ Devices
- **Brian Stein**, CH2M HILL
- **Abel Sussman**, Booz Allen Hamilton
- **Dr. Robert Yen**, Booz Allen Hamilton
- **Mike Zercher**, NXP Semiconductors

About the Identity Council

The Identity Council is focused on promoting best policies and practices concerning person and machine identity, including strong authentication and appropriate authorization across different use cases. Through its activities, the Council encourages the use of digital identities that provide strong authentication across assurance environments through smart credentials—e.g., smart ID cards, mobile devices, enhanced driver's licenses, and other tokens. The Council furthermore encourages the use of smart credentials, secure network protocols, and cryptographic standards in support of digital identities and strong authentication on the Internet.

The Council addresses the challenges of securing identity and develops guidance for organizations so that they can realize the benefits that secure identity delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organizational resources to bear on addressing the challenges of securing identity information for proper use.

Additional information on the use of smart card technology for identity applications can be found on the Smart Card Alliance Web site at http://www.smartcardalliance.org.

8 Appendix A

Table 4 summarizes how the use of smart card technology can add value to any authentication solution.

Table 4. Value Added to Authentication Solutions by Smart Card Technology

Authentication Mechanism	Issue	Value Added by Smart Card Technology
Single-Factor Authentication		
Static password	▪ Easy to guess, sniff, or steal ▪ Difficult to enforce strong password policies ▪ User frustration and resistance to changing and memorizing passwords ▪ Cost to manage	A smart card system provides a secure container for passwords and automates the user's logon, relieving the user of the requirement to manage passwords. Strong password policies are easy to enforce.
Passive or active device without a PIN	▪ Device loss or theft	A smart card system provides security for the device seed and also adds PIN-based access to the card, implementing two-factor strong authentication.
Biometric	▪ Replay attack ▪ Masquerade attack ▪ Biometric credential and matching security ▪ Online database connectivity requirement (unless used with smart card) ▪ Theft of database – biometrics cannot be revoked	A smart card system provides secure storage for the biometric template, performs the biometric match on the card (enabling an offline authentication process), and adds PIN-based access to the card, implementing three-factor authentication.
Two-Factor Authentication		
One-time password with PIN	▪ Complex infrastructure ▪ Man-in-the-middle attack ▪ Single function product ▪ OTP seed protection ▪ Token life-cycle cost	A smart card system replaces a single-function device with multi-function capability (securing application and network access) and reduces overall complexity and life-cycle cost. Investment can be leveraged by using the card as a smart ID badge for secure building access. Smart cards are programmable. Cards can be reused easily, supporting a more cost-effective approach to issuing temporary access cards. New smart card functions can be added after issuance, supporting upgrades to systems or new applications

Authentication Mechanism	Issue	Value Added by Smart Card Technology
Biometric and password	▪ Complex back-end infrastructure ▪ Credential security ▪ Online database connectivity requirement ▪ Theft of database – biometrics cannot be revoked	A smart card system provides secure storage for the biometric template and performs the biometric match on the card (enabling an offline authentication process).
Three-Factor Authentication		
Device, biometric, PIN	▪ Credential security, whether on a server or workstation ▪ Complex infrastructure ▪ Online database connectivity requirement ▪ Theft of database – biometrics cannot be revoked	A smart card system provides the least complex mechanism for three-factor authentication when integrated with biometric match-on-card capability. There is no requirement for connection to a database.