Smart Card
Alliance

Strong Authentication Using Smart Card Technology for Logical Access

A Smart Card Alliance Access Control Council White Paper

Publication Date: November 2012

Publication Number: ACC - 12002

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

Smart card technology has advanced over the last 30 years: storage and processing capabilities are improved, security has been enhanced, the management software has matured, contactless technologies are available, and multiple applications can now be integrated on a card. Smart cards now support a variety of the logical access applications used by organizations, including network logon, one-time passwords (OTPs), virtual private network (VPN) authentication, e-mail and data encryption, digital signatures, enterprise single sign-on, secure wireless network logon, and biometric authentication. Today, smart cards can play an essential role in the security backbone of an organization's identity management architecture, supporting the strong authentication required to validate individuals accessing networked resources and providing a critical first step in protecting against intruders.

1.1 Authentication Overview

In general**,** authentication is the process by which something is shown to be genuine. In this white paper, the term is applied to the identity of a person (though it can also be extended to things) and, by extension, to the items used to prove that identity to an electronic system, such as background documents, user name-password combinations, smart cards, or biometric data.

The authentication method used and the extent to which it is applied depends on the subject being examined. For example, different measures are employed to authenticate a $1 bill as opposed to a bill of a much higher denomination. Similarly, a different method is used to authenticate someone who is requesting access to a product technical support web site as opposed to someone accessing secure government or military networks.

Where minimal security is required (such as on a home computer that is not connected to the Internet), a simple logon name may be sufficient. Requiring authentication, such as a personal identification number (PIN) or password, adds a level of protection. This combination provides minimal authentication and can be supplemented or replaced by requiring other authentication tokens, such as digital certificates, hardware-based authentication tokens, or biometric data.

The strength of any authentication process depends on both the quality and diversity of its constituent parts. To build greater integrity into a solution, the authentication methods should employ complementary mechanisms. Historically, these mechanisms have included something a person knows (a password), possesses (an object), or is inherent to their physiology or behavior (a biometric factor).[1] The concepts of uniqueness and secrecy are very important in this context. Although location data and knowledge-based authentication can limit the potential for fraud within a system, as currently implemented they provide only a limited degree of uniqueness and secrecy, respectively.

1.2 Authentication Drivers

Changes in the business environment can represent strong drivers for IT processes and for implementing stronger authentication. The increasing number and popularity of e-commerce business applications, the migration to cloud-based systems, critical requirements by employees and customers for remote information access, and the move to bring-your-own-device implementations, all argue for ensuring that strong authentication is in place for every transaction. Protecting both an organization's information and the customer's information is critical, for a number of reasons:

[1] Commonly referred to as "something you know, something you have, something you are."

- Numerous businesses are currently trying to comply with new or changing regulatory mandates, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, Visa Waiver Program, or International Civil Aviation Organization Machine-Readable Travel Documents specifications.

  Many of these mandates affect policymakers as well as IT departments. Stronger authentication methods can help address mandated requirements for access and audit trails.

- Many organizations or their business partners have suffered from a security breach, or an audit has uncovered vulnerabilities.

  Such events can be costly and unpleasant, but they can provide the motivation to justify implementing stronger security measures. Analyzing these events for weaknesses in current authentication procedures permits organizations to apply stronger authentication methods to their current systems.

Many organizations are implementing centralized identity management systems, moving to cloud-based solutions or implementing bring-your-own-device strategies. This IT infrastructure migration provides opportunities for organizations to also implement stronger authentication processes to protect critical business resources and address governance, risk management and compliance objectives. The remaining sections of this paper describe strong authentication and discuss identity proofing, identity credentials, and authentication factors, providing examples of authentication tokens and factors. The paper then explains why smart card technology, by design, empowers strong authentication and provides some example use cases.

2 Identity Proofing and Identity Credentials

Identity proofing is the method by which an individual proves their identity to an identity provider and the identity credential issuer.[2] The identity proofing process requires significant human involvement and takes a long time. Therefore, rather than repeating the effort for each logical or physical access attempt, the relying party issues a credential that links to a digital identity for the individual and that can be electronically validated for future access requests.

An identity proofing process of some kind occurs millions of times every day for people across the globe. Throughout the course of their lives, most people hold multiple identity credentials, each with a different purpose and a different renewal schedule.

The certainty with which this identity must be proven is determined by the relying party and is likely to be related to the risk of allowing access inappropriately and the threat of attacks on the identity proofing process. Commonly the identity proofing process can include the following activities:

- Presentation of identity documentation (e.g., birth certificate, passport)
- Verification of documentation (where appropriate)
- Confirmation of approval to access information or facility
- Positive vetting of the individual's identity (i.e., background check), if a very high level of assurance is required
- Biometric data capture (either for identity proofing, duplicate registration rejection, or inclusion as an authentication token)
- Issuance of the credential (frequently as a badge or hardware token, such as a smart card)
- Personalization and activation with creation of a PIN or password

An identity credential is a tangible object, a piece of knowledge, or a sample of a person's physical attributes that may be used during the process of confirming an individual's claimed identity. In addition, a credential may be used as an attestation of qualification, competence, or authority issued to an individual by a third party.

A credential may be used by an individual requesting access to a given physical facility or information system. The combination of a user account number or name and a secret password is a widely-used classic example of IT credentials. Typically, credentials can be something you know (such as number or PIN), something you have (such as a card access badge), something you are (such as a biometric feature) or some combination of these items.

Credentials are objects that bind an identity to a token. Token form factors vary widely and include contact and contactless smart cards. An increasing number of information systems also rely on an object or data structure (e.g., X.509, public key certificate) that authoritatively binds an identity to a token possessed and controlled by an individual. To maintain the level of assurance provided by an electronic authentication solution, credentials and tokens should be managed to reflect any changes in that binding.

[2] The registration process for the U.S. Federal Government PIV involves multiple source documents, fingerprint capture, in-person identity proofing (twice), and completion of minimum background investigations before the individual is given the PIV smart card identity credential. See National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, FIPS 201, for details on the specifications.

As an example, the U.S. Federal government Personal Identity Verification (PIV) card is defined by FIPS 201 as a physical artifact (e.g., a contact and contactless smart identity card) that contains stored credentials such as a photograph, cryptographic keys, digitized fingerprint representation, and is issued to federal employees and contractors. The claimed identity of the individual cardholder may be verified by electronic, or visual, comparison of the biometric credentials stored on the card.

The quality of an identity credential is often determined by a combination of a *level of assurance* (which attests to the rigor of the identity proofing process) and a *level of authentication* (which is used to verify the identity at the time of a transaction).

Identity proofing and the process by which an identity credential is issued are the cornerstones of strong authentication. Using more than one identity proofing procedure increases the level of assurance that a person is who that person is claiming to be. Table 1 lists examples of identity proofing procedures used in the government, financial, higher education, and corporate sectors.

Table 1. Examples of Identity Proofing Procedures

Identity Proofing Category	Example
Remote	Confirmation of an e-mail address by receiving an e-mail and confirmation code Confirmation of a mobile device by receiving either a text message or a phone call with a confirmation code Confirmation of an address by receiving a letter with a confirmation code
In person	Presentation and validation of a government-issued identification credential (driver's license, passport, Social Security number) Biometric data capture and validation Presentation of non-government credentials (healthcare card, credit card)
Knowledge based	Knowledge of historical financial or utility information Knowledge of previous addresses as provided by credit reporting agencies Knowledge of educational transcript details

2.1 Derived Credential

A "derived credential" is a credential that is issued based on a previously issued credential, created for use in a different application and/or in different form factors. This section discusses an example of a derived credential based on the Federal PIV credential.

A derived credential in a smart mobile device could be issued upon presentation and validation of a PIV card. This option requires the PIV card to be presented to a mobile device manager (MDM) which then assigns the derived credential to a smart mobile device, a new logical credential being stored within the mobile device. The credential would typically be placed on a secure element within the mobile device (e.g., a secure element in the UICC/SIM, in a microSD card or in a separate embedded chip). The derived credential differs from the PIV card in that it may not necessarily be used where PIV cards are normally accepted; it is independently revocable; any associated card authentication key (CAK) identify it as mobile; and it could imply different levels of security and authority. The derived credential would also be revoked by default when the PIV credential from which it was derived is revoked.

In addition to mobile devices, derived credentials could take the form of other smart cards and tokens for use on laptops and desktops, and for Web access. Derived credentials are in the process of being standardized by NIST. FIPS 201-2 refers to a future NIST special publication, SP 800-157 (Guidelines for Personal Identity Verification (PIV) Derived Credentials), that will provide guidelines on PIV derived credentials.

These new specifications accommodate two important new use cases, allowing the issuance of back-up credentials and the issuance of credentials on alternate, non-card form factors and in mobile devices. PIV derived credentials are not PIV credentials, but may be used in lieu of PIV credentials for the same access applications. The concept of a derived credential described in NIST SP 800-63-1, Electronic Authentication Guidance, introduces guidelines that permit leveraging an existing credential to issue derived credentials. A derived credential is defined in NIST SP 800-63-1 as "a credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process."

Further, NIST SP800-63-1 states the following regarding level of assurance (LoA):

- Derived credentials from the *same* credential service provider (CSP) cannot exceed the assurance level associated with the original credential.
- Derived credentials from a *different* CSP must be less than the assurance level associated with the original credential.[3]

2.2 Examples of Identity Proofing and Credential Issuance

This section describes examples of different identity proofing and credential issuance processes.

As a first example, Alice requests an account for an online business networking site. As part of the registration process, Alice must provide an e-mail address. The networking site sends a verification code to that e-mail address. Alice must enter the code in a form on the networking site before she is provided a user name and password for ongoing access. This registration process does not prove that Alice is indeed Alice and not someone else, and does nothing to validate that Alice deserves access to the site. The process only proves to a reasonable level of assurance that Alice is a person, rather than an automated system, and that she has a valid e-mail address. The identity credential that Alice is issued is her password.

Next**,** suppose Alice is hired by Company A. She must be interviewed in person by a company representative, show her birth certificate or passport, have her picture taken, and verify her permanent address (place of residence) by presenting a letter that Company A mails to her permanent address. After going through this registration process, Company A gives Alice a badge with her picture on it, which permits her to access a Company A building for work. To logon to Company A computers, she is issued a user name and password. For remote log-on, such as from her house, Alice is issued a Universal Serial Bus (USB)-based smart card with public key infrastructure (PKI) credentials and PIN protection.

This registration process proves that Alice is indeed Alice, that she lives at a specific address, that she is legally entitled to work, and that she is a real person. This is referred to as an identity proofing encounter. The established identity and background investigation is used during the adjudication process that determines if a credential should indeed be issued to Alice. In this

[3] A special case allows issuance of new LoA 4 credentials if the CSP can collect and verify a biometric.

example, the identity credentials Alice is issued are the company badge, the password, and a USB smart card with associated PIN.

Later, Alice requests a credential that will be stored and maintained on her mobile device. The request is approved by the company and since Alice has already been issued a USB smart card credential, the company policy allows issuing an additional credential without having to repeat the full identity vetting process.

In this example, if Alice is a Federal employee and has a PIV credential, she must demonstrate that she is in possession and control of her original credential, and that she is biometrically bound to the chain-of-trust established during the issuance of the previous credential. If this is done remotely, PIV policies allow the original issuer to provision up to LoA 3 derived credentials. If Alice appears in person and is in possession of the original credential, PIV policies allow the issuing authority to provision up to LoA 4 derived credential.

3 Authentication Factors and Authentication Tokens

It is important to understand what authentication factors are and how they relate to identity credentials and authentication tokens. This section describes the factors used in authentication processes and the types of tokens that may be used for authentication.

When selecting the number of authentication factors and the authentication token to use, only a thorough vulnerability and risk assessment and cost-benefit analysis can accurately predict the best implementation. When all assessments are complete, the results should point developers to the appropriate implementation.

3.1 Authentication Factors

Authentication factors confirm that a person is who that person claims to be. There are three standard categories of authentication factors:

- An ownership factor, or something you have
- A knowledge factor, or something you know
- An inherence factor, or something you are

The evidence a person provides to support each factor is called the *authentication token*.

Table 2 lists the three categories of authentication factors and examples of candidate tokens.

Table 2. Authentication Factors and Example Candidate Tokens

Factor	Token
Something you have	▪ An authentication token stored on a smart card based ID card ▪ An authentication token stored on a USB device ▪ An OTP device, such as a smartphone ▪ A private key in a public–private cryptographic key pair
Something you know	▪ A password or PIN ▪ A knowledge-based question such as "mother's maiden name"
Something you are	▪ Biometric data, such as a facial image, fingerprint, voice print, or iris (eye) scan

Not all electronic systems or identity credentials use all three authentication factors. Using more than one authentication factor increases the strength of the authentication. Multi-factor authentication is a form of layered security; it is unlikely that multiple factors will be disabled by someone using a single type of attack. Multiple factors would have to be compromised for authentication to be compromised.

Table 3 summarizes single and multi-factor authentication with examples. The following sections describe a variety of authentication tokens that can be used as proof for authentication.

Table 3. Single- and Multi-factor Authentication Examples

Authentication	Description	Example
Single factor	The person provides one authentication token for one factor.	Alice is required to know her password.

Authentication	Description	Example
Multi-factor	The person provides more than one authentication token for one or more authentication factors.[4]	Alice is required to know both her password and her mother's maiden name.
Two-factor	A person provides at least one authentication token for two different authentication factors.	Alice is required to have her USB-based PKI smart card token and present it to the system when using her home computer. To unlock the USB-based smart card, Alice is required to know her PIN.
Three-factor	A person provides at least one authentication token for three different authentication factors.	Alice is required to have her USB-based PKI smart card token and present it to the system when using her home computer. To unlock the USB-based smart card, Alice is required to know her PIN. To login to the computer, Alice is also required to submit a biometric (e.g., a fingerprint).

3.2 Authentication Tokens

3.2.1 Passwords

The most commonly used authentication token is the password. Someone provides a user name and password and requests access. A computer system compares the user name and password combination to stored information. An electronic response grants or denies access based on the results of this comparison.

Passwords have been widely recognized as a weak form of authentication[5], with increasing amounts of password theft, either directly from the owner, through network intrusion, or through unauthorized database access. Passwords are typically controlled by the password owner, who can select easily guessed passwords, share passwords with others, write passwords down, use the same password to access multiple systems, or inadvertently compromise the password as the result of a phishing attack. In addition, storing password data on corporate networks introduces additional vulnerability should attackers gain network access.

Private enterprises and government agencies are moving to replace simple passwords with stronger, multi-factor authentication that strengthens information security, responds to market and regulatory conditions, and lowers support costs.

3.2.2 Knowledge Based Authentication Tokens

Knowledge based authentication (KBA) uses personal information to validate someone's identity electronically. KBA can be used to identify someone accessing an information system, service, or Web site.

KBA can be deployed statically or dynamically. Static KBA implementations generally use various combinations of stored information that someone provided earlier. The implementation

[4] Multi-factor authentication is sometimes misunderstood to only refer to two-factor and three-factor authentication. Multi-factor authentication also includes the use of multiple tokens for one-factor authentication as in the example given.

[5] See NIST SP 800-63-1, Appendix A: Estimating Entropy and Strength for additional information.

can obtain the information from one or multiple systems, smart cards, and services. However, all shared information to be used for identity verification must have been recorded earlier (i.e., sensitive data that is shared prior to use). This shared personal information is sometimes referred to as "shared secrets." Dynamic KBA implementations can enhance the level of verification, because they do not rely on prearranged shared information for authentication. Instead, the system can use information acquired on the fly, from (for example) smart cards, public records, marketing data, or credit reports. Likewise, dynamic KBA implementations can change shared information rules dynamically.

The choice of a static or dynamic KBA implementation should be made with proper due diligence.

3.2.3 Public Key Cryptography and Digital Certificates

Public key cryptography (also known as asymmetric key cryptography) encrypts information using mathematically related pairs of cryptographic keys. One key in the pair is used to encrypt information; the information can then only by decrypted using the other key. The key pairs are obtained from a trusted authority and used to exchange data securely and privately.

Each key pair comprises a public key and a private key. The public key is used to encrypt confidential information. The private key authenticates the key holder and decrypts information that has been encrypted using the public key. The private key must be kept secret. The recipient using the private key can therefore be certain that the information the key is able to decrypt was intended for them, and the sender can be certain that only the holder of the private key can decrypt the information sent.

Smart card technology provides a portable platform where the asymmetric key pair can be generated and securely stored in the card. Private key cryptographic functions are performed on the card and the key cannot be revealed, exported or copied. In addition, a smart card is capable of binding the card to the card owner and the public key to the card. As another benefit, several laptop manufacturers are offering smart card readers as a standard feature in their products.

Certificate-based smart cards using PKI can provide strong multi-factor authentication in a traditional ID card form factor. Smart cards with two-factor authentication provide high assurance identification and authentication to applications and networks where security is critical. Smart cards offer a single solution for strong authentication and logical access applications including network access, remote access, password management, network logon, as well as corporate ID badges for identification, physical access control, and payment systems. Further, certificate-based smart cards can achieve the highest security standards including FIPS 140-2 and Common Criteria, and enable compliance with other security regulations and guidance, including Homeland Security Presidential Directive 12 (HSPD-12), Federal Identity, Credential, and Access Management (FICAM) guidance, Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act.

3.2.4 One-Time Passwords

A one-time password (OTP) can combine the factors of something a person knows (e.g., a passphrase) and something a person has (e.g., possession of a token). An OTP displays a single use password. Each time a person authenticates to a system, a different password is generated and used, after which that password is no longer valid. The password is computed either by software on the computer system or by OTP hardware tokens in the person's possession that are coordinated through a trusted system. One common implementation model is for the password to be generated by a portable device such as a USB device, smart display card, or mobile phone.

OTPs were developed to combat the problems encountered in using personally-selected static passwords and managing password security policy. The key to a successful OTP solution is that each OTP is different from the previous one, and the sequence of OTPs cannot be guessed based on observation of previous passwords. These methods are designed to protect against "man in the middle" and other attacks.

Some popular implementations use short message service (SMS) to send a code to a person's mobile phone as part of the authentication process. As long as the USB device, token, smart display card, or mobile phone remains with the person, ownership factors constitute strong evidence of a user's identity.

One-time passwords are usually determined by HMAC-SHA-1, HMAC-SHA-512 or HMAC-SHA-256 hash algorithms. Multiple types of OTPs are available: event-based, time-based and challenge/response algorithms. The Initiative for Open Authentication, (OATH)[6] has developed three algorithms that have been standardized by the Internet Engineering Task Force (IETF): HOTP, event-based, RFC 4226; TOTP, time-based, RFC 6238; and OCRA, challenge/response, RFC 6287.

Typically, OTP technology can support strong, two-factor authentication, in which individuals demonstrate something they know (a user name-passphrase combination) and something they have (the device generating the OTP).

3.2.5 Biometrics[7]

Biometric factors, or something you are, are an important component of multi-factor authentication. Biometrics bind an individual to an asserted identity both during the identity credential registration process and during the authentication event.

Biometric technologies measure a person's physical or behavioral characteristic. A biometric measurement begins with the collection of a digital biometric sample (e.g., bitmap image) using a sensor device. Useful features contained in the collected sample are then extracted and formatted into a template record that can be matched against other template records. The template is stored at registration (and when combined with identity vetting, establishes an identity). When a transaction takes place, the same biometric characteristic is measured, processed into a template format, and compared to the previously registered template.

Virtually all biometric measurements will vary slightly from one measurement to the next. This variation is not typically due to changes in the biometric feature being measured but to the mechanism and environment in which the data are captured. Therefore, a biometric sample measured at registration will not precisely match the results of the live sample measurement. As a result of this variability, a similarity score is generated and this score is compared against a pre-determined threshold setting to determine what constitutes an acceptable match.

[6] http://www.openauthentication.org/

[7] Additional information on biometrics can be found in the Smart Card Alliance white paper, "Smart Cards and Biometrics," available at http://www.smartcardalliance.org/pages/publications-smart-cards-and-biometrics.

4 What Is Strong Authentication?

Strong authentication currently has no precise definition; it is not a strictly mathematical concept with purely quantitative measurements, but rather a qualitative measure with a relative scale. For example, the government's Personal Identity Verification (PIV) smart card program outlines the following levels of authentication assurance:

- Some confidence: a basic degree of assurance in the identity of the cardholder
- High confidence: a strong degree of assurance in the identity of the cardholder
- Very high confidence: a very strong degree of assurance in the identity of the cardholder.[8]

"Strong" generally means better than what has traditionally been acceptable. For electronic systems, strong authentication goes beyond the typical user name-password combination and other simple, single-factor authentication methods. "Strong authentication" provides a higher level of confidence in the identity of the individual.

Measuring authentication strength typically means dealing with multiple considerations that combine to yield an overall measurement. These considerations include:

- The number of factors employed in the authentication method
- The number of tokens for each factor
- The strength of each token (i.e., whether the identity credential or authentication tokens used can be compromised or circumvented)

The number of factors employed is an important consideration. Additional factors significantly improve the overall strength of authentication. Strength is also a function of the strength of the individual factors employed. A PIN, a password, or your mother's maiden name each has different actual (and sometimes perceived) strength. For example, a typical 4-digit PIN is considered to be weaker than an 8-character password that uses upper- and lowercase letters. One reason is because the two tokens have different lengths. Another reason is that the two tokens have a different number of possible permutations (i.e., for the PIN, the number of permutations is 10^4 with 4 digits of 0-9, as opposed to a password with just 8 lower- and uppercase letters, for which the number of permutations is 52^8). The password is substantially stronger than a numeric PIN: the chances of guessing the PIN are 1 in 10,000 chances, as opposed to 1 in 53,459,728,531,456 chances of guessing the password. Other examples are less clear: in requiring your mother's maiden name as opposed to your favorite dog's name, the length of the names is a factor that yields equivalent strength, as do the uniqueness or obscurity of the name. Those measures are much more difficult to quantify; hence, the non-absolute determination of overall strength for some factors.

The use of cryptography in strong authentication should be based on sound cryptographic principles and use of keys of appropriate strength.

Finally, an authentication method is typically considered to be strong if the following are true:

- At least two of the three authentication factors are used.
- The cost, computing power, and time required by a determined attacker to attack an authentication token exceeds the value of compromising the token and the related asset.
- The identity vetting and proofing requirements applied when issuing the identity credential can reasonably assert that electronic Alice is, in fact, Alice.

[8] National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, FIPS PUB 201-1, March 2006.

5 Smart Cards and Strong Authentication

Smart cards can significantly increase the security of a person's identity credentials. The credentials can be permanently stored on the card, which is in the person's possession. In addition, sophisticated attacks on smart cards are time-consuming and expensive, and the attacker must have physical possession of the card. If a person's smart card is missing, it is likely that the person will report it, and the card can be revoked and re-provisioned before an attack can succeed. When credentials are stored on someone's computer, that person may never know that they have been stolen.

5.1 Authentication Factors Enabled by Smart Cards

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

Smart card technology also supports the addition of biometric tokens (something you are), enabling three-factor authentication. As an alternative, the biometric can replace the PIN, which strengthens security while increasing convenience. Adding biometric authentication to an access control solution is easy, because the smart card can store the cardholder's biometric template and perform the processing required to check for a match. No back-end database is required. Storing the credentials for accessing an application securely on a smart card, protected by the cardholder's biometric data, provides an organization with biometric security without having to involve back-end applications.

5.2 Form Factors

Smart card technology 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. Each implementation incorporates a computer chip that can carry a microcontroller, crypto-coprocessor, memory, operating system, and application software. Microcontroller-based smart cards are designed to resist attack using a variety of countermeasures built into the chip by the manufacturer, making it less likely that data stored on the smart card will be exposed, stolen, modified, or destroyed.

Mobile devices, especially smartphones, offer multiple opportunities for implementing smart card technology. An SE can be embedded directly in the device or held on the universal integrated circuit card (UICC), also known as the subscriber identity module (SIM). Many phones have the ability to read microSD cards, which constitute another possible form factor. The evolution of Near Field Communication (NFC) technology within the mobile sphere has sparked considerable interest in using smartphones in authentication processes.

Using a smartphone with an SE as the form factor for strong authentication and for storing identity credentials can have the following benefits:

- Market penetration
- A "constant companion" for users
- Technological maturity
- Touchscreen capability for entering data, such as passwords
- Integral secure cryptographic processing capability
- Capability to use certain biometrics (e.g., voice) without the added cost of a reader

- Ability to serve as both the provider and reader of identity credentials
- Ability to enable advanced, novel interactive applications
- Location-based verification applications

Regardless of form factor, smart cards can be used to implement any of the authentication techniques described in this white paper.

5.3 Advantages of Smart Cards

Smart cards offer the following advantages:

- Secure password file storage
- Ability to generate asymmetric key pairs and store PKI certificates securely
- Secure symmetric key storage
- Secure OTP seed storage
- Secure biometric template storage

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

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

Authentication Mechanism	Issue	Value Added by Smart Card Technology
Single-Factor Authentication		
Static passwords	▪ 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.

Authentication Mechanism	Issue	Value Added by Smart Card Technology
Two-Factor Authentication		
One-time password device 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. Smart card 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
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.

In summary, using smart cards can provide the following advantages:

- Support for multiple applications and sets of application data on the card
- Support for cryptographic authentication tokens and use of digital signatures for strong audit functions
- Support for multiple types of authentication tokens, providing redundant features for identity authentication and security for the identity information and identity authentication process
- Support for offline authentication processes
- Secure storage of biometrics and other credentials (e.g., PINs)

6 Use Cases for Strong Authentication with Smart Card Technology

Many industries use smart card technology for strong authentication. This section describes three different use cases for smart card technology-based strong authentication:

- Enterprise employee identity credential
- Consumer online banking identity credential
- Patient and provider healthcare cards
- Transit use of a smart identity credential

6.1 Enterprise Use Case

Company A hires an employee, and the employee undergoes pre-employment screening, as required by Company A's policy. The employee provides fingerprint scans and historical and biographical information. The fingerprint scans are submitted to a third party for a background investigation and are also converted to ANSI 378 minutiae templates for use in access control.

Upon completion of a successful background check, drug screening, and any other employment prerequisites, the employee visits Company A's human resources (HR) department, where a fingerprint match is performed to assure that this is the same person. A smart card is personalized with the biometric template, access control identifier, picture, and other printed and encoded information. The card management system (CMS) issues a digital certificate, which is used to digitally sign all data encoded on the card. Additionally, the employee is allowed to select a PIN that is not to be shared and that meets minimum complexity requirements. This PIN is stored and maintained within the smart card.

The access control identifier, employee name, access privileges group, and other information is sent to the physical access control system (PACS) and the logical access control system (LACS). Physical and logical access privileges can now be defined further according to corporate policy and procedure.

Many physical and logical access points are secured against unauthorized access by a requirement for strong authentication. Logical access control processes for the corporate applications that require authentication (typically a user name and password) are upgraded to recognize the smart card. The employee needs only to enter the card PIN to logon. In addition, smart card readers at access-controlled doors validate the card, using the stored digital certificate, before granting whatever access the privileges allow. Access control points to areas protected by additional security (such as corporate servers and file rooms that include personally identifiable information or any other corporate sensitive data) also validate the PIN and perform a biometric match.

Company A can create a self-service intranet portal, where employees who have forgotten their passwords can answer some static knowledge-based questions and submit fingerprint scans to have their PINs reset.

When Company A terminates an employee, the HR system sends a communication to the LACS and PACS to invalidate the card identifier. At the same time, the CMS revokes the digital certificate. This combination provides multiple routes for invalidating a card in all corporate systems.

6.2 Online Banking Use Case

Increasing counterfeit card fraud led the financial industry to move to smart chip technology for bank cards and to develop the global EMV specifications[9] for bank cards based on chip card technology. The EMV specifications, first available in 1996 and managed by EMVCo, define the global interoperable standard for smart bank cards 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 issuance. According to EMVCo,[10] approximately 1.5 billion EMV cards have been issued globally and 21.9 million POS terminals accept EMV cards as of Q2 2012.

In the UK, 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 the MasterCard 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 associated with their account into the offline reader.
2. The reader prompts the cardholder to enter the cardholder's 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 eight 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. This development is a significant improvement over accounts protected only by user names and passwords, which are 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 this kind of attack than those with more comprehensive and 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

[9] 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.

[10] http://www.emvco.com. 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. With the acquisition of Europay by MasterCard in 2002 and with JCB and American Express joining the organization in 2004 and 2009, respectively, EMVCo is currently operated by American Express, JCB International, MasterCard Worldwide, and Visa, Inc.

solution achieves the goal of enhanced security while maintaining processes that are simple, convenient, and easily adopted by banking customers.

6.3 Healthcare Card Use Case

Healthcare organizations can benefit by using smart card technology to provide authenticated access to medical information and identities. The use cases in this section illustrate how smart cards are used to implement strong identity authentication and information security with the following benefits:

- Compliance with the Health Insurance Portability and Accountability Act (HIPAA)
- Implementation of portable medical records
- Medical identity theft mitigation
- Accessible emergency medical information
- Administrative cost reduction
- Healthcare provider identification credentials
- Healthcare fraud reduction

The actors in these use cases include healthcare providers, support associates, insurance providers, and patients.

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.

6.3.1 HIPAA Compliance

Healthcare organizations are required by HIPAA to safeguard patient health information to protect the security and confidentiality of each individual's 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.

6.3.2 Portable Medical Records

Numerous pilots and applications have demonstrated the use of smart cards for implementing portable medical records and secure and controlled access to distributed repositories of patient health records and insurance data. The card can also contain pointers to larger medical information repositories, such as detailed medical histories, medical images, x-rays, and insurance information.

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

6.3.3 Medical Identity Theft Mitigation

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

A multi-factor authentication solution that identifies the patient, the medical provider, and all others handling patient information can span data locations, maintain privacy, and facilitate the secure exchange of medical information. A smart card identity solution can be a cost effective, secure, and user-accepted method for reducing or preventing identity theft.

6.3.4 Emergency Medical Information

Emergency personnel and first responders need immediate information about patient medical conditions and allergies. Making emergency information available using smart cards and portable readers can enable first responders to manage and coordinate life-saving information at any location: at the site of an emergency, during patient transfer, or within the healthcare facility's emergency room.

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.

Storing critical data on smart cards improves patient-to-responder communication and effective treatment delivery. A patient's blood type, allergies, and medications can be stored in a standard and easily accessible format for immediate use and transmission to a waiting emergency department staff. In situations in which patients cannot speak for themselves, smart healthcare cards can provide life-saving information. Such information should include but need not be limited to the following:

- Patient identification and demographic information
- Blood type
- Allergies
- Medications
- Conditions, treatments, and prescriptions

Other on-card information can include a living will, organ donor and insurance information, religious preferences, and emergency contact information.

6.3.5 Administrative Cost Reduction

Increasing financial pressure on healthcare service delivery is forcing administrators to monitor all administrative costs.

Healthcare organizations can use smart card technology to maintain patient data, increasing returns on investment, improving care, and lowering staff costs. The secure data storage capabilities provided by smart cards can streamline paperwork and reporting. Providers, insurers, and retail healthcare markets can realize improved returns on investment by using smart cards.[11]

[11] Additional information on the cost savings of smart healthcare cards can be found in the Smart Card Alliance white paper, "A Healthcare CFO's Guide to Smart Card Technology and Applications," available at http://www.smartcardalliance.org/pages/publications-healthcare-guide-smart-card-technology-applications.

6.3.6 Healthcare Provider Identification Credential

Identification, authentication, and authorization are the pillars of security for electronic information. As healthcare providers migrate from paper to electronic medical records, 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. With the use of large clinical data exchanges, it is critical that user privileges be assigned using role-based access controls and use smart cards and multi-factor 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. Access areas can include the pharmacy (employee restricted), 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 multi-factor authentication and the cryptography capabilities supported by smart cards can provide benefits in the form of stronger identity verification and can help to assure corporate network security.

6.3.7 Healthcare Fraud Reduction

Healthcare fraud and abuse have a negative effect on healthcare organizations, increasing delivery costs and curtailing patient care. Although only a small percentage of healthcare providers and consumers deliberately engage in healthcare fraud, even modest levels of fraud can increase the costs of healthcare for everyone.

Implementation of an online and offline smart card-based prescription and service delivery auditing program can reduce healthcare fraud. If a physician or pharmacist is offline, the smart card can retain medical data until the next time the card can communicate with the online system. Insurance eligibility and prescriptions can be verified by either or both systems. In this case, data and access audits are accurate and up-to-date. This use of smart cards can also expose dishonest providers and consumers submitting false or misleading information for healthcare benefits determination.

6.4 Transit Use Case

A card-based identity credential issued for employee or student identification can also be used in applications such as transit.

For example, the Federal Personal Identification and Verification (PIV) card could be used in a transit environment to validate the rider's credential that is associated with a closed transit account-based system that supports and maintains a prepaid funding source such as federal transit benefits.

To access prepaid transit benefit funds, a PIV card unique number is securely captured and maintained by the transit enrollment system using the card's contact interface. That unique number is then associated with an account earmarked for transit benefit funds specified by the PIV card issuing agency that maintains the actual personally identifiable information relating the credential to the user.

In order to acceptably conduct a secure fare payment transit transaction using a federally-issued PIV card, the contactless interface must also be secured between the card and the fare payment acceptance terminal while ensuring that the total transaction time does not exceed 300ms. In this environment, the capability of secure messaging enables data transmitted between the card and a correctly-configured reader to be both integrity-protected and encrypted. Once secure messaging has been established, a virtual contact (i.e., contactless) interface may be utilized.

If a PIV card has been revoked or lost/stolen and a replacement card reissued, the new card must be reregistered in the transit system. The status of all registered PIV cards is periodically checked by the transit agencies using PKI certificate validation.

It is expected that some federally issued PIV cards will also be configured with an alternative open loop payment application for in-area parking and/or out-of-area transit fare payment. This functionality will be capable of initiating standard secure contactless payments using EMV retail payment methodology. In this case, a private funding source must be used and standard banking relationships apply. Further use of the PIV card for merchant category codes other than transit would be determined by agency policy and banking business relationships.

7 Summary

Organizations globally are moving to strong authentication solutions for authenticating identities prior to granting access to computer networks, systems and applications. Factors driving this move include changes in the IT infrastructure (e.g., cloud-based computing that provides increased public exposure), requirements to protect systems and information from increasingly sophisticated attacks, and regulatory mandates for securing information and protecting employee, patient and consumer privacy.

The identity assurance process consists of multiple steps. An individual must prove their identity; a credential is issued; the credential asserts proof of identity for authentication. Multiple authentication factors are used with a variety of authentication tokens.

Strong authentication is not precisely defined, but is a qualitative measure with a relative scale. Strong authentication for logical access means going beyond the typical user name-password combination and simple single-factor approaches. The strength of "strong" authentication depends on the number of factors employed, the strength of each token, and the potential that the authentication token was compromised or circumvented.

Smart card technology provides an excellent platform for implementing strong authentication. Smart cards securely support all of the authentication tokens, storing password files, PKI certificates, one-time password seed files, and biometric image templates, as well as generating asymmetric key pairs. A smart card used in combination with one or more authentication tokens provides stronger multi-factor authentication and significantly strengthens logical access security. Smart card technology also provides the flexibility for including all authentication tokens in a single smart card, improving the security and privacy of the overall authentication process. A single smart card can be used for authentication for both physical and logical access.

In addition, smart cards can support a variety of applications used by organizations, including Windows logon, password management, one-time passwords (OTP), VPN authentication, e-mail and data encryption, electronic signatures, enterprise single sign-on, secure wireless network logon, biometric authentication, personal data storage, role-based access, and secure physical access. Today, smart cards are essential to the security backbone of an organization's identity management system, supporting the strong authentication required to validate individuals accessing networked resources.

8 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Access Control Council to discuss the benefits of using smart card technology for strong authentication for logical access.

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

The Smart Card Alliance thanks the Council members for their contributions. Participants involved in the development of this white paper included: AMAG Technology; Consult Hyperion; Damalas LLC; Gemalto; GSA; HID Global; HP Enterprise Services; IDentification Technology Partners; Identive Group; IDmachines; IQ Devices; NagraID Security; NXP Semiconductors; Oberthur Technologies; Roehr Consulting; SAIC; U.S. Department of Defense/Defense Manpower Data Center (DoD/DMDC); U.S. Department of State.

The Smart Card Alliance thanks the following Council members who contributed to writing, editing and reviewing this white paper:

- **Tim Baldridge**, Dept. of Defense
- **Sal D'Agostino**, IDmachines
- **Tony Damalas**, Damalas LLC
- **Bob Dulude**, HID Global
- **Michel Escalant**, Gemalto
- **John Esser**, Oberthur Technologies
- **Margaret Ford**, Consult Hyperion
- **Marty Frary**, Independent Consultant
- **Bob Gilson**, DoD/DMDC
- **Walter Hamilton**, ID Technology Partners
- **Daryl Hendricks**, GSA
- **Lolie Kull**, HP Enterprise Services
- **LaChelle LeVan**, Consultant
- **Don Malloy**, NagraID Security
- **Cathy Medich, Smart Card Alliance**
- **Neville Pattinson**, Gemalto
- **Roger Roehr**, Roehr Consulting
- **Steve Rogers**, IQ Devices
- **Dan Schleifer**, IDmachines
- **Adam Shane**, AMAG Technology
- **Mike Sulak**, Dept. of State
- **Lars Suneborn**, Hirsch-Identive
- **Joe Tassone**, Identive Group
- **Chris Williams**, SAIC
- **Mike Zercher**, NXP Semiconductors
- **Rob Zivney**, ID Technology Partners

About the Access Control Council

The Smart Card Alliance Access Control Council is focused on accelerating the widespread acceptance, use, and application of smart card technology for physical and logical access control. The group brings together, in an open forum, leading users and technologists from both the public and private sectors and works on activities that are important to the access control community and that will help expand smart card technology adoption in this important market.

9 Appendix A: Examples of Organizations Using Smart Card Technology for Logical Access

The following are examples of organizations in North America who are using smart cards for authentication for logical access applications. This list is not intended to be exhaustive but to provide examples of organizations that have moved to smart card technology.

- Boeing
- Booz Allen Hamilton
- Deloitte
- Eastman Chemical
- Executive Branch of the U.S. Government (Personal Identity Verification (PIV) program)
- Gemalto
- Lockheed Martin
- Microsoft
- Northrop Grumman
- SAIC
- Schlumberger
- Sun Microsystems / Oracle
- University of Central Florida
- Virginia Tech
- Wells Fargo Bank
- XTec, Incorporated