Secure Identification Systems: Building a Chain of Trust

A Smart Card Alliance Report

Publication Date: March 2004

Publication Number: ID-04001

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

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, health care, retail and entertainment industries, as well as a number of government agencies. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. For more information, visit www.smartcardalliance.org.

Table of Contents

Introduction

Security is currently one of the most demanding requirements in our society. The challenge is simple: how to protect what belongs to you. "You" can be a business, government agency, or individual person. What belongs to you can be a tangible asset, such as a physical object, or an intangible asset, such as information, rights, or privileges. But in all cases, such assets have significant value to the owner.

Virtually everything against which assets require protection involves people. Digital and physical attacks are all created and carried out by people. It is therefore essential to be able to clearly and accurately identify those who should have access to what belongs to you and allow them access. Everyone else should be rejected. Such identification capabilities are carried out by a secure identification (ID) system.

Essential to a secure ID system is a *chain of trust*. Trust in processes, people, architecture and technologies is vital to building and having confidence in a secure ID system. A chain of trust guarantees the authenticity of the people, issuing organizations, devices, equipment, networks, and other components of a secure ID system. The chain of trust must also ensure that information within the system is verified, authenticated, protected and used appropriately.

This report examines the elements that are essential to creating and maintaining a chain of trust:

- The trust model adopted within an organization or among organizations that participate in an identification system
- The processes used to verify that people are who they say they are and enroll them in the identification system
- The process that validates identities and identity credentials
- The architecture, technologies, and processes that keep identity information private and secure and ensure accurate identity verification
- The system management functions that maintain the chain of trust

The use of smart ID devices, especially in the form of smart cards, offers advantages for both physical and logical security. Smart cards are a vital link in a chain of trust. They can provide secure and accurate identity verification and, when combined with other ID system technologies (such as biometrics and digital certificates), they can enhance the security of the system and protect the privacy of system information.

This report introduces the challenges faced by ID systems and discusses the elements that are key to implementing a secure ID system. It outlines enrollment, issuance and identity verification processes and issues. The report describes the role smart cards play in the chain of trust for a secure ID system, discusses smart card implementation considerations, and summarizes how smart cards can help to address the key vulnerabilities of current ID systems.

The power and portability of the smart card, well-designed system architecture and strict operating procedures combine to form a reliable and controllable chain of trust for secure ID systems.

How Today's Identification Systems Can Fail

Today, nearly everybody carries multiple identification cards (IDs), issued by multiple public and private organizations. Such IDs include driver's licenses, membership cards, credit cards, and corporate identification badges.

The primary purpose of an ID is to identify the holder as having particular rights, privileges, and responsibilities. IDs verify a person's identity, both to the system that issued the ID (for example, a driver's license verifies the license-holder's right to operate a motor vehicle) and to other systems that do not issue their own IDs (for example, a driver's license verifies the identity of someone trying to board an aircraft).

Systems that issue IDs are typically one of two types:

- Systems that interface with citizens, such as a driver's license system, citizen entitlement system, or passport system. Such systems are *citizen-facing systems*.
- Systems that interface with employees or customers, such as an employee badge system, human resource benefits system, or online banking system. Such systems are *employee- or customer-facing systems*.

Regardless of type, many of today's identification systems are vulnerable. They often use tamper-prone credentials or easily compromised passwords that are insufficient to stand up against the sophistication of modern identity thieves. To be secure, identification systems must meet multiple challenges.

Table 1 identifies the top issues and challenges facing current ID systems and describes the issues for both citizen-facing and employee- or customer-facing systems.

Table 1: ID System Issues and Challenges

Issues and Challenges	Citizen-Facing Systems	Employee- or Customer-Facing Systems
Many of today's ID systems fail to provide adequate security and privacy	• Recent terrorist attacks point out the need for more security. • Identity theft has become a major problem in entitlement systems. • Cyber-terrorism is an emerging threat to many citizen-facing systems.	• 88% of businesses have been victim of cybercrime according to a July 2003 survey by CSO magazine. • Datamonitor reports that worldwide IT security breaches cost companies about $15 billion per year.
Establishing the initial identity of ID system members can be difficult	• Legitimate persons can have unreliable or missing identity documentation. • Persons can easily obtain counterfeit or fraudulent identity breeder documents. • Identity theft often starts with a thief using a genuine breeder document to get a legitimate ID.	• Employers encounter job applicants who misrepresent their identities when seeking employment. • In customer-facing systems, businesses often have minimal background information to establish customer identity.
Identity is not sufficiently verified in most ID systems today	• Many citizen-facing systems use weak forms of identity verification, such as Social Security numbers or driver's licenses. • There are more than 300 valid forms of government-issued IDs in the U.S., making it very difficult to distinguish between genuine and fake IDs. • Identity verification is often limited to the observations or discretion of the government officer checking the ID.	• Over 90% of companies use passwords as the primary method of access control to information resources. • Passwords represent significant security risks because they are typically controlled by the user who can: - Use easily guessed passwords. - Share passwords with others. - Write passwords down. - Use the same password across multiple systems.

Issues and Challenges	Citizen-Facing Systems	Employee- or Customer-Facing Systems
Identity credentials can be difficult to issue and manage for large member populations	• Large citizen populations present unique challenges such as relocations, births, deaths, and changes of status. • Many government systems operate large numbers of service locations and must manage staffing challenges such as training and turnover, as well as control the security risks of issuing IDs from multiple sites.	• As employees and applications within an enterprise increase, issuing and managing IDs become more difficult for both administrators and users. • A Meta Group study indicates that about one-third of help desk calls request password resets. It also found that companies delete accounts for only about 70% of ex-employees.
Different systems require their own identity documents, causing members to need multiple IDs	• Different governments often require their own IDs for citizens within their jurisdiction. • Even within a given jurisdiction, different government agencies may require citizens to obtain multiple IDs, such as a driver's license, voter ID, and social services ID.	• Employees often carry multiple IDs to access company facilities and other IDs to access computer networks. • Employees and customers must remember multiple usernames and passwords, making it likely that they will re-use passwords or use easily remembered passwords.
Many ID systems are proprietary and inflexible, making them difficult to change and grow	• Current systems are usually bounded by the issuing agency's or government's jurisdiction, making it difficult for systems to cooperate and collaborate across jurisdictions. • Few standards apply across government systems (for example, driver's licenses). Where standards do apply (for example, passports), they have not yet been universally adopted.	• Traditional enterprise ID systems require users to manage identities by application, which is expensive and difficult to maintain. • Newer, Web-based systems adhere to standards and allow user identities to be shared across enterprise applications. However, non-Web applications prevail in most organizations, preventing ID consolidation.
The convergence of physical and logical security places new demands on today's ID systems	• Citizen-facing systems have traditionally used IDs only to confirm physical identity. As e-government initiatives grow, the need to provide for cyber identity is becoming critical to systems. • Government systems are being asked to move to more sophisticated ID technologies to meet both physical and logical security needs.	• More and more organizations recognize the potential advantages of an integrated view of security, but the cultural differences between the physical and logical security domains present a challenge to this integration. Additional technologies are needed to join these two worlds and streamline both functions.
Current ID systems are expensive to operate and support	• Many systems rely on manual processes and are labor intensive. • Many systems are operated by contractors, requiring extensive replacement or turnover when contracts expire.	• The Aberdeen Group found that the cost of configuring and maintaining password systems for small companies averages $100-$150 per user per year. Costs for a mid-tier company average $200, and a large enterprise spends an average of $300-350 per user per year.
Current ID systems are plagued with usability problems	• Users must often apply for new or duplicate IDs when moving to a new jurisdiction. • Users must often deal with long wait times and poor customer support.	• Users must juggle too many IDs on a daily basis. • Most of today's ID systems fail to alleviate administrative overhead, consolidate user credentials, and close security holes.
There is little or no apparent ROI for enhancing current ID systems	• Most systems are based on user fees for revenue. IDs are a cost to these systems. • Government-issued IDs are often accepted by other agencies. While improvements can benefit multiple systems, return on investment is hard to calculate across multiple agencies.	• Enterprises have invested in firewall and virtual private network technologies to keep intruders out, but have invested little in strong user identity verification. • Most companies today want to see a return on investment in 6 months or less, which can inhibit investment in ID system enhancements.

What Makes an Identification System Secure

A secure ID system is designed to address one primary requirement: verify that an individual is who the individual claims to be. When properly designed, secure ID systems implement a chain of trust, assuring everyone involved that the individual presenting an ID card is the person who owns the credentials on the ID and that the credentials are valid. (The term "credential" refers to information stored on the card that represents the individual's identity document and privileges.) A secure ID system can provide individuals with trusted credentials that are used for a wide range of applications, from enabling access to facilities or networks to proving entitlement for services to conducting online transactions.

Critical to any secure ID system is the ID card.[1] The ID card is used as a portable, trusted and verifiable representation of an individual's identity and rights and privileges within the ID system. For an ID card to meet these requirements, the ID system must assure that a legitimate authority issued the ID, that the ID and the credential it carries are not counterfeit or altered, and that the person carrying the ID matches the individual who enrolled in the ID system.

The Secure ID System Trust Model

Secure ID systems can be implemented within a single group, across multiple groups within an organization or enterprise, or among multiple organizations and enterprises. Regardless of the number or type of entities involved, however, to be truly secure, ID systems must implement a trust model. The trust model institutionalizes commonly held principles and policies: system operations always have the same outcome, regardless of where they are performed, and all parties involved can trust that the system accurately and securely verifies identities. Before implementing any system, all entities participating in an ID system must define and agree to a trust model.

When an organization is implementing an ID system only for its own employees to access its resources, the trust model can be relatively straightforward. But some systems rely on a single ID card to verify identity across multiple organizations (for example, across government agencies or organizations, between business partners, or between commercial and government entities). Establishing trust in such a system (i.e., *a federated identity system*) can be complex.

The *federated identity trust model*[2] is an example that is being implemented among multiple organizations, both in government and industry. This trust model was designed to allow participants in a federated identity system to have a shared authentication infrastructure using a common trust level. This model provides the foundation for policies that guide secure ID system operating rules and business procedures and is especially relevant for systems that involve multiple, independent organizations.

---

[1] This report refers to the physical ID device as an "ID" or "ID card." While ID systems may issue different physical ID form factors, a plastic card that incorporates other technologies used in identity applications (e.g., chip, barcode, magnetic stripe) is the prevalent form factor for a secure ID system.

[2] Additional information about how the federated identity trust model is being used can be found at http://www.fegc.org/pilotInfo.htm.

For example, organizations that allow "outsiders" to access their facilities require extensive security procedures. The greater the number of outsiders with access, the more complex the procedures. One challenge is to verify that a visitor from another organization is the expected visitor. Another is to authenticate the visitor's identity, verifying that the visitor is who the visitor claims to be. Even if the visitor can be verified as an employee of the visiting organization, unless both organizations have adopted a common process for establishing identity, one organization may unwittingly grant access to a person of questionable background.

One way to ensure security in such a federated system is to establish a common set of policies and rules for proving and authenticating the identity of people who visit another organization's facilities and to require that all organizations commit to these rules. However, if more than two organizations are involved, multiple bilateral agreements are required, resulting in complex trust management. In this situation, an intermediary can be established. This intermediary is often referred to as the "trust broker."

A trust broker implements business requirements shared by the organizations involved in a federated identity system, obligates those organizations to adhere to the rules and procedures established to meet these requirements, and processes identification authentication inquiries from the system members. In a federated identity system, establishing and maintaining the validity of the trust relationships among the entities involved translates into two high-level requirements:

1) Adherence to procedures used to verify a person's identity prior to issuance of a credential
2) Authenticating identities whenever individuals present themselves to the ID system

Design Elements that Make an ID System Secure

Secure ID system design requires a set of decisions that select and implement policies, procedures, architecture, technology, and staff. The design must implement the desired level of security and the appropriate chain of trust, with the authentication process incorporating appropriate security measures and technologies to deter impersonation and counterfeiting and assure the privacy of the credentials on the ID.

The design of a secure ID system must include the following:

- A secure enrollment process that establishes each individual's identity and determines that the person is entitled to the privileges that are being granted
- Procedures for securely issuing ID cards and ensuring that IDs are issued only by authorized issuing organizations and only to the correct person
- Policies and procedures for monitoring the use of the ID
- Procedures for ID life-cycle management
- Training for users and issuers
- Policies, procedures and technologies that protect access to the information in the system about ID holders
- Security controls that provide only authorized viewers with access to information on the ID
- An authentication process that implements the defined chain of trust, verifying the identity of ID holders and the legitimacy of the ID cards and their credentials

Components of a Secure ID System

Table 2 lists the components required by most secure ID systems and provides examples of the types of decisions that must be made to select each component.

Table 2: Secure ID System Components

Component	Key Design Decision
Trusted Issuing Authority	‣ What trust model organizations participating in the ID system should adopt ‣ What types of digital credentials to use and what security algorithms to implement ‣ Whether to use a commercial trusted authority to create, protect, and distribute certificates or create certificates in house, in a protected environment ‣ What the key management processes are
Network and Infrastructure	‣ Whether communications should be distributed or centralized ‣ How to implement trusted channels ‣ How to design secured environments ‣ How to issue credentials: locally, regionally, or centrally ‣ How to protect individuals' privacy and safeguard their personal information ‣ How to distribute trusted materials ‣ How to control and manage system access
Enrollment Stations	‣ The environment and location of enrollment stations ‣ What method to adopt for operator self-authentication ‣ What method to adopt for verifying the credential applicant's identity ‣ How stations should interact with the network
Issuance Process	‣ What the ID personalization process should be ‣ How to be sure the distribution process complies with the defined security policy ‣ How to implement ID inventory physical security ‣ How to audit ID cards ‣ How to implement data security ‣ What the life-cycle management process should be
ID Credential / Card	‣ What types of applications to support, now and in the future ‣ What the ID card will look like, what information should be on it, whether anti-counterfeiting and anti-tampering features are needed, whether a photo or other biometric is needed ‣ How often the ID should be used and under what conditions ‣ The type of ID technology ‣ The security certification level
Cryptography	‣ Which encryption technology to select ‣ Whether to implement symmetric or asymmetric keys ‣ How many keys to issue and what key space size is desirable
Biometrics	‣ Whether to use biometrics (e.g., fingerprint, facial, iris scan) ‣ What algorithm to use to process biometric information ‣ How many biometric measurements to store and where to store them ‣ Under what conditions to use biometrics
ID Readers	‣ Location, number, and architecture of ID readers and how to protect them ‣ Design and appearance of the readers ‣ How the ID should authenticate the readers ‣ How to manage security features and security certification level ‣ How to implement secure communication with the network ‣ What processes to use to manufacture readers

Privacy Requirements for Secure ID Systems

In addition to protecting an organization's assets, secure ID systems must also protect the privacy of the individuals enrolled in the system and safeguard their personal information. Privacy requirements are a key issue for successful implementation of a secure ID system.

To be considered "privacy-enabled," an ID system must satisfy the following requirements:

- Control the collection, use, and release of personal information
- Protect each individual's right to control how personal information is collected and promulgated
- Protect against identity theft and the use of an individual's personal information for fraudulent purposes
- Protect the confidentiality, integrity, and availability of information that identifies or otherwise describes an individual

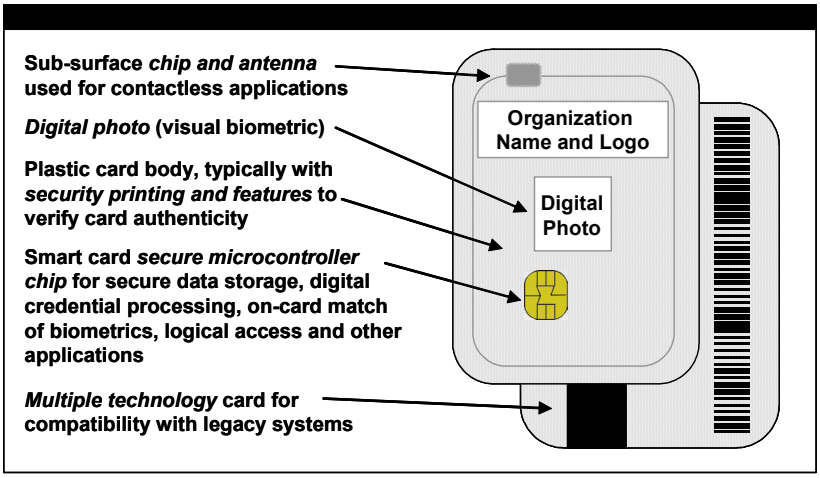
A number of government organizations and industry groups have developed recommendations for fair information practices and guidelines to protect individual privacy. System designers need to consider business practices, security policies, and system architectures, as well as technologies, in developing a privacy-enabled system.

Smart Cards and Secure ID Systems

Smart cards are widely acknowledged as one of the most secure and reliable forms of electronic identification. A smart card includes an embedded computer chip that can be either a microcontroller with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless electromagnetic interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader.

A smart ID card can combine several ID technologies, including the embedded chip, visual security markings, magnetic stripe, barcode and/or an optical stripe. Figure 1 illustrates components on a typical smart ID card. Many government organizations and enterprises are now implementing smart card-based secure ID systems for physical and logical access and adding other applications that have traditionally required separate identification processes and cards. Appendix A includes profiles of several organizations who are implementing smart card-based secure ID systems.

Figure 1: Smart ID Card Example



Secure Identification System Enrollment

A critical link in the chain of trust for a secure ID system is a secure enrollment process. Enrolling someone improperly (whether through intentional fraud or mistake) negates the purpose of the system and creates a potentially dangerous situation that can be difficult and costly to correct.

Three Elements of Security

Individuals typically prove their identity to ID systems using a single indicator. However, effective identity authentication requires the use of a combination of three indicators, or factors, including:

- **Possession.** The individual is in physical possession of an item such as keys, a driver's license, an identity card, or a passport.
- **Knowledge.** The individual knows information such as a password, secret code, or personal identification number (PIN) that can only be known by that individual.
- **Characteristics.** The individual demonstrates a unique physical quality or behavior that differentiates the individual from all other people.

For a large scale ID system implementation, each of the 3 elements must be usable by the vast majority of individuals. The enrollment process must capture the appropriate information to support all of the factors needed by the ID system to verify identity.

The Enrollment Process

A secure enrollment process must be well planned to avoid fraud and to make the process as seamless as possible. Enrollers need to be trained and educated to understand their roles, the characteristics and functions of the ID card, and the importance of enrollment. Enrollees must prove their identity. Enrollee information must be checked to ensure that the person has not already enrolled as someone else, possibly with different demographic data.

The information used to identify and enroll individuals must be of the highest quality (for example, demographic data must be complete, photo images must be clear and sharp, and biometrics must be accurate). ID holders must be educated during the enrollment process, not only on enrollment but also on the use of the ID. Lastly, the process must ensure the ID holder's privacy.

How Individuals Prove Their Identity

Individuals currently prove their identity using various methods, ranging from low security (for example, "self assertion" or a mail-in application) to high security (for example, in-person identification or a third-party database check).

One common method of verifying identity during the enrollment process is to require an individual to present one or more *breeder documents*. A breeder document is any document that can be used to obtain additional identity documents.

Depending on the ID system enrollment process, a breeder document can be a birth certificate, a Social Security card, or something as simple as a utility bill. For example, a state may offer an identity card to all state residents that can be used to obtain discounts at certain retailers, ride public transportation

at a reduced rate, cash checks, or purchase liquor. In some cases these documents can be obtained with minimal verification of the information provided. Such a card can then be used as a breeder document to obtain other identity credentials. Some of the September 11th terrorists were able to obtain driver's licenses in Virginia using these types of breeder documents.[3]

An enrollee's identity can be proved with more confidence by incorporating additional checks into an enrollment process, such as a third-party database check. The enrollment process results in the individual's identity being tied to the factors that are used to authenticate identity in the ID system (for example, a password, biometric, ID card or digital certificate), carrying the chain of trust forward.

ID System Use of Biometrics

New secure ID system implementations are requiring one or more biometrics to provide increased assurance that an individual presenting the ID card has the right to use that ID. Biometrics are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics. The common types of biometrics and the distinctive characteristics on which they are based are as follows:

- Fingerprint, based on the unique friction ridges on the finger surface (the most widely used biometric)
- Facial, based on the location and composition of distinctive features of the face and their interrelation
- Iris, based on the ridges, furrows, and striations that characterize the ring around the pupil
- Voice, based on spoken phrases
- Hand geometry, based on the height, width, and structure of the hand and fingers
- Retinal, based on patterns on the rear of the eye
- Signature, based on the speed, stroke order, and pressure derived from a written pattern

Printed biometric information, such as photographs, height, weight, eye color, and hair color, has been used for years to authenticate identity. These simple biometrics are verified visually. However, visual verification is a subjective process, and the inspector can be fooled (for example, if a valid ID is used by an impersonator). In addition, an enrollee may not provide accurate information originally (e.g., incorrect weight, wrong eye color) or the ID holder's appearance may have changed since enrollment.

Issues with Enrollment and ID Production

When developing an enrollment system, care must be taken to ensure that the system gathers quality data quickly and accurately. It is important to craft the enrollment process so that it is straightforward for the enrollment personnel and both frustration-free and educational for the enrollee. This will help to ensure user acceptance of the ID card and associated technologies, which are likely to be new to the ID holder. Where appropriate, educating the user about how and where biometric templates are stored and used can

[3] As a result, Virginia has improved identity verification processes and most states are looking at improving their procedures for verification of identity prior to issuing an ID. A summary of the American Association of Motor Vehicle Administrators' efforts to improve identification security can be found in Appendix A.

ease concerns about privacy. For example, a smart card is used in some ID systems, with biometric templates stored exclusively on the card and accessed only if the user presents the card to an authorized system. ID system users who initially express concerns are often reassured when they learn how such a system works.

When biometric information is used, the data captured must be of the highest quality. Poor quality information can decrease system performance and produce false negatives, frustrating users and necessitating reenrollment. Many software packages indicate the quality of the captured biometric. Organizations should decide on a minimum level of quality and have procedures for repeating enrollment if sufficient quality is not achieved. An important aspect of capturing quality biometrics is the instruction given to the enrollee prior to capture. For many enrollees, the enrollment process will be their first exposure to a biometric system; therefore, proper instructions, practice, and feedback are critical. It may be advisable to allow first-time enrollees to do a sample enrollment with verification prior to actual enrollment. This will allow enrollees to become accustomed to the system. Consideration should be given to allowing the enrollee to see the on-screen results of the sample and actual enrollment.

In addition, using biometrics in an identification system can impose additional interface requirements. For example, systems that have one-to-many biometric-matching capabilities can present multiple potential matches for human verification. Operators typically cannot verify an individual's identity based on the biometric images alone, but if the biometrics are accompanied by photographs, identification by an operator is possible.

When enrollment is implemented electronically, an enrollee's ID card can be produced either centrally or at the enrollment location. Cards produced locally can be given to the user within minutes. Centrally produced cards must also be delivered to the cardholder securely.

Regardless of where an ID card is produced, counterfeiting is an issue. Security can be enhanced by using special laminates and cryptographic measures for cards that store electronic data. Technologies such as laser perforation, which might not be practical for local production, can protect cards produced centrally from counterfeiting attempts. Centralized production can also simplify control of card stock and laminate.

Replacement of lost and stolen cards is also an issue. An appropriate card management system can "hot-list" cards reported as missing and issue a replacement card without requiring reenrollment. When a hot-listed card is read by a device that is hot-list enabled, the card can be disabled, confiscated, or ignored, as appropriate.

ID Use, the Chain of Trust and the Role of Smart Cards

The chain of trust for a secure ID system encompasses all of the system's components and processes, assuring that the system as a whole is worthy of trust.

This section describes the chain of trust that is required to authenticate an individual's identity and ensure the validity of the ID and credential once the ID has been issued and is in use. To illustrate the strongest possible chain of trust, the discussion assumes that the ID includes an electronic device (or chip) embedded in a personal portable document (for example, an electronic passport) or in a card.

What Contributes to a Chain of Trust

The chain of trust when using an ID in a secure ID system assures the following:

- The ID holder is the correct and valid user of the ID.
- The ID holder has authorized the release or use of the ID credential for identity verification.
- The ID credential presented is valid (i.e., genuine, unaltered and not expired) and is from the authorized issuer.
- The ID (e.g., passport or smart ID card) is valid, is not counterfeit and is appropriate for the ID credential being carried.
- The electronic device carried by the ID is valid and not counterfeit.
- The external device reading the ID is authentic and trusted.

This chain of trust requires a number of steps and processes to provide assurance of the identity verification process.

Physical ID Verification

Identity authentication typically begins with verifying the physical ID itself. IDs can be physically verified in different ways. The method chosen should be appropriate for the level of confidence required. Methods include:

- Examination of an ID held by the user but not surrendered (such as a flash pass)
- Examination of an ID that is surrendered by the user
- Inspection by a machine of unique data elements stored on or in an ID (such as a bar code) or comparison of an ID to a reference template

In all cases, the ID being presented is checked visually or electronically for specific details that indicate its authenticity. The details can take the form of one or more security features, such as:

- Correctness of topographical information
- Visual validity/expiration date
- Security printing (for example, microprinting)
- Embedded optical security devices, such as holograms and optically variable devices or optically variable or ultraviolet inks
- Security laminate over printed information
- Correctness of construction
- Photograph of the document holder
- Machine-readable passive media (for example, bar codes or optical characters)

ID Device Authentication

To ensure that the electronic device used on the ID being presented is authorized and not fraudulent, the device is typically authenticated electronically using symmetric shared secret keys, asymmetric public/private keys or one time password (OTP) authentication. Electronic verification is accomplished using a device that can "read" the ID. The authentication process may be accomplished between the ID and the reader or may require the reader to communicate with a host system or authentication server.

Device authentication using a symmetric shared secret key. To authenticate an ID using a symmetric shared secret key, both the ID device and the reader must know a common (shared) secret key. The reader presents the device with a challenge which must be encrypted in some manner with the shared secret key. The result is sent from the ID device to the reader and verified against an independent calculation performed by the challenger. If the results match, the ID is assumed to be authenticated. A variation is to add message authentication codes (MACs) to all messages; these provide the strongest authentication when the MAC is computed in real-time based on a challenge from the reader.

Device authentication using asymmetric public/private keys. This mechanism relies on the ID device generating an asymmetric public/private key pair, with the public portion available to all parties needing to verify the device authenticity. When a reader wishes to challenge the ID, it can present a challenge for the device to digitally sign using its private key. When the device returns the signed data, the reader can then verify the digital signature from the device using the device's public key. A variation of this technique requires the ID to sign a block of data or message, which is transmitted to external equipment in real time.

One time passwords. One time passwords serve as dynamic authentication credentials that have a very limited life to prevent common static password-based attacks. OTP-based authentication comes in two forms – either synchronous, where both the device being authenticated and an authentication server must act in congruous fashion, or asynchronous or challenge-response, where data is securely exchanged between the device and an authentication server.

Reader Authentication

Symmetric shared secret keys can also be used to authenticate the reader to the ID. In this case, the ID would issue a challenge to the reader and verify the result with an internally calculated value. Without a satisfactory response, the ID device will not release any of its credential content. This technique is used to prevent counterfeit readers from being able to steal credential information that could then be used to make counterfeit IDs.

ID Credential Authentication

The digital credentials stored on the ID card can be authenticated using an issuer's digital signature or message authentication code. In this case, the credential authentication is typically based on static data. Other techniques must be used to ensure that the information has not been cloned or otherwise compromised or is not being presented in a replay attack. An additional complication is that the reader must also be able to determine when the credential expires.

ID Holder Authentication

The person holding an ID can be authenticated in two ways, by checking:

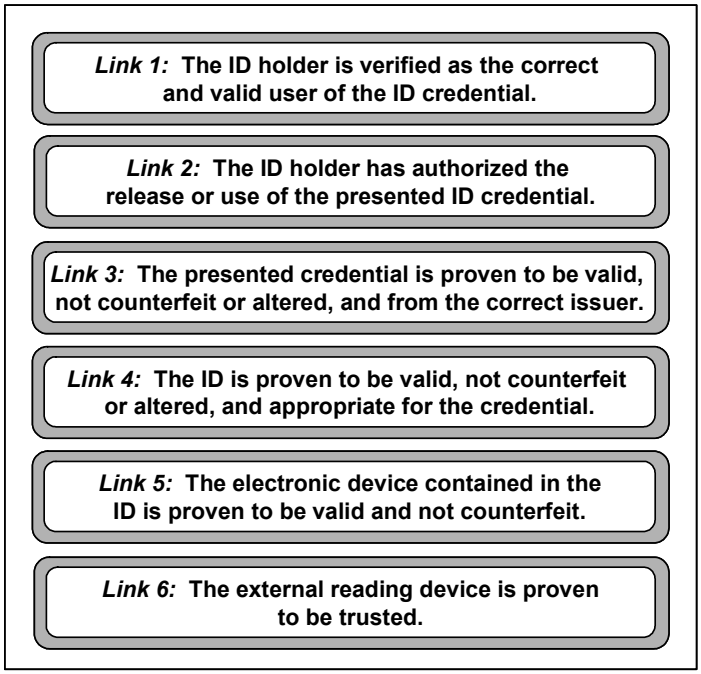
- What the user knows (for example, a PIN or password), and/or
- What the user is (for example, a biometric).

Entering a PIN or password indicates to the electronic device on the ID that the user is present. This allows the device to release the ID holder's identity credential or allow its use.

To check "what the user is," either the photo on the ID card is compared to the face of the presenting ID holder or an automated biometric match is done. Biometric-based ID systems capture a "live" biometric image (for example, a fingerprint or hand geometry scan) and compare it to the stored biometric image that was captured when the individual enrolled in the system. This biometric one-to-one match verifies that the ID holder is the same person who enrolled in the ID system and is the correct person to use the ID. Biometrics can also protect access to the credentials on an ID.

Figure 2 summarizes the key links in the secure ID system chain of trust during the identity authentication process when the ID is used.

Figure 2: The Chain of Trust during ID Usage



The Role of Smart Cards in the Chain of Trust

Smart card technology can strengthen many of the links in the chain of trust in a secure ID system. Smart cards can act as the individual's ID card and allow secure access to information and services in both online and offline system designs. With the ability to store, protect and modify information written to the on-card electronic device (i.e., chip), smart cards offer unmatched flexibility and options for information sharing and transfer, while providing the unique ability to incorporate privacy-sensitive features.

Support for Physical and Digital Identity. Smart cards provide the unique capability to easily combine identification and authentication in both the physical and digital worlds. This can generate significant savings as the smart card-based ID card could not only be used to allow physical access to services, but also allow individuals to file taxes, request official papers (e.g., a birth certificate) online, or access secure networks.

Authenticated and Authorized Information Access. The information required to identify an individual typically depends on the individual's role in the situation. For example, when cigarettes are being purchased, the only identification information required may be the individual's age. Whether the individual can drive and where the individual lives may be irrelevant.

The smart card's ability to process information and react to its environment gives it a unique advantage in providing authenticated information access. A smart card is able to release only the information required and only when it is required. Unlike other forms of identification (such as a passive printed driver's license), a smart card does not expose all of an individual's personal information (including potentially irrelevant information) when it is presented.

Strong ID Card Security. When compared with other tamper-resistant ID cards, smart cards represent the best compromise between security and cost. When used with other technologies such as public key cryptography and biometrics, smart cards are almost impossible to duplicate or forge and data stored in the chip can't be modified without proper authorization (a password, biometric authentication or cryptographic access key).

Smart cards can also help to deter counterfeiting and thwart tampering. Smart cards include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. Where smart ID cards will also be used for manual identity verification, visual security features can be added to a smart card body.

ID Credential Security. Protecting the privacy, authenticity, and integrity of the data encoded on an ID as credentials is a primary requirement for a secure ID system. Sensitive data is typically encrypted, both on the smart ID card and during communications with the external reader. Digital signatures can be used to ensure data integrity, with multiple signatures required if different authorities create the data. To ensure privacy, applications and data on the card must be designed to prevent information sharing.

System Component Authentication. For the most robust security and privacy, the secure ID system may require that system components authenticate the legitimacy of other components during the identity verification process. The smart ID card can verify that the card reader is authentic, and the card reader in turn can authenticate the smart ID card. The smart ID card can also ensure that the requesting system has established the right to access the information being requested.

Smart Card Support for Privacy Requirements. The use of smart cards strengthens the ability of a system to protect individual privacy.[4] Unlike other identification technologies, smart cards can implement a personal firewall for an individual, releasing only the information required and only when it is required. The card's unique ability to verify the authority of the information

[4] For additional information on how smart cards can enhance privacy in an ID system, see the Smart Card Alliance white paper, "Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology," available at www.smartcardalliance.org.

requestor and its strong card and data security make it an excellent guardian of the cardholder's personal information. By allowing authorized, authenticated access only to the information required by a transaction, a smart card-based ID system can protect an individual's privacy while ensuring that the individual is properly identified.

Smart Cards and Biometrics. Secure ID systems that require a high degree of security and privacy are increasingly implementing both smart card and biometric technology. Smart cards and biometrics are a natural fit to provide two- or multi-factor authentication. A smart card is the logical storage medium for biometric information. During the enrollment process, the biometric template can be stored on the smart card chip for later verification. Only the authorized user with a biometric matching the stored enrollment template receives access and privileges.

Chain of Trust Summary

Any ID system must define the appropriate security goals and attributes in a security policy. This policy must identify the security that is appropriate and commensurate to the value of each asset being protected. When developing this security policy, careful attention should be given to the strength of each link in the chain of trust when using the ID card and credential. To the degree that the system will rely on visual or manual verification, adequate attention must be given to training for anyone who must make decisions on ID card and credential authenticity, and policies should be in place to address failures to follow procedures.

A robust and complete chain of trust for an ID card and credential is mandatory for a secure ID system. With the advent of smart cards, electronic devices that store ID credentials, and biometric verification, the level of trust for a credential being presented can be significantly increased. The electronic device (e.g., a chip in an electronic passport or smart ID card) is the portable digital security agent of the issuer and is a vital link in the chain of trust for any serious secure ID system.

Business and Implementation Considerations for Smart Card-Based Secure Identification Systems

How Organizations Build the Business Case for Smart ID Cards

Physical and information security is a paramount concern for organizations of all sizes and in all industries. Every organization must determine the risks of potential security breaches and quantify the potential costs of such breaches. The results of this risk assessment can indicate whether investing in enhanced physical and information technology (IT) security makes good business sense.

The amount of investment that an organization makes in security technology should be proportional to the value of the assets that are being protected. Therefore, the organization should base its risk analysis primarily on the required level of security. Security investment tends to have diminishing returns. The organization will need to determine how much it is willing to spend for 1% or 5% of additional security.

Business Case Factors
• Reducing the risk of security breaches and their resulting costs (e.g., financial, productivity, sales, market position, legal exposure)
• Complying with legislation and regulations
• Reducing current operating costs
• Solving operational business problems
• Improving productivity
• Enhancing user convenience

Another factor to consider is the potential impact of legislation and policy on the business environment in which the organization operates. For example, there is now an enormous push to improve cybersecurity in both the public and private sectors, driven primarily by the federal government and the Department of Homeland Security. Legislation passed in the last few years requires federal agencies to ensure that their networks are secure and that access to them is controlled and monitored. These government requirements will probably be extended into the private sector, so that businesses working with the government will have to demonstrate that they do not constitute a "weak link" in the security chain. Businesses are also subject to a number of new requirements for access control and audit as a result of new laws or regulations such as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the U.S. Patriot Act.

Any risk analysis should also examine how improved security and authentication technologies could reduce current operating costs and solve operational business problems. An organization can start its return on investment (ROI) analysis by examining the costs of managing passwords. The proliferation of networks and applications has increased the costs of password management and support for users who forget passwords or don't comply with password policies. The opportunity costs of wasted time and lost productivity and the telecommunications charges incurred in resetting passwords can be used to develop a good estimate of baseline costs. An organization can then begin to calculate the impact on these costs of implementing a secure ID program that supports strong authentication and single sign-on applications.

The institution of a smart card-based secure ID platform could have other financial benefits. Such a platform can enable new applications with a positive impact on solving business problems, saving money, and increasing

user convenience. For example, many organizations could use an electronic purse application on a smart card to replace cash-based cafeteria or vending machine services. Using an electronic purse reduces the costs of handling cash, delivering cost savings to an organization's food service operation. The smart card platform can also support secure and portable data storage, which can enable automated form filling applications and digital signing capabilities, eliminating the need for paper forms and the costs related to printing, storage, and handling.

The business case analysis should include a determination of what the organization currently pays to sustain multiple ID programs (for example, parking cards, door access cards, cafeteria cards, computer logon cards). The organization should examine the costs incurred by using multiple card systems, each with a single function and administration and overhead costs, as opposed to adopting a single smart card-based system that supports multiple functions and requires a single administrative support team. Table 3 suggests possible applications that can be implemented on a multi-application smart card.

The result of the business case analysis should be a quantifiable ROI and time to breakeven.

Table 3: Example Applications for a Multi-Application Smart ID Card

Physical access	‣ Environment: campus, single building, parking lot ‣ Interior: entrances, lobbies, offices, computer rooms, vaults ‣ Transportation: buses, planes, trains, ships, subways
Logical Access	‣ Network: LAN, WAN, signed and encrypted e-mail, secure transactions ‣ Common files: shared/working documents, employee handbook, newsletters ‣ Confidential files: payroll, trade secrets, human resource files
Data Storage	‣ Property management ‣ Clearance information ‣ Personnel rosters ‣ Medical information ‣ Training/certifications ‣ Personal information for electronic forms submission
Financial	‣ Electronic purse: cafeteria, transit, parking ‣ Credit or debit payment
Privilege Management	‣ Healthcare ‣ Voting ‣ Driver's license ‣ Travel/border crossing ‣ Electronic benefits
Law Enforcement	‣ Criminal records ‣ Citizenship ‣ Immigration status ‣ User/document authenticity confirmation ‣ Identification at time of death

Implementation Considerations for Issuing ID Cards

Implementation of a secure ID system should focus on how to meet the following requirements:

- Collecting and handling all card data/demographics securely.
- Managing the storage of card data securely and with attention to privacy issues.
- Delivering IDs to end users promptly and efficiently.
- Controlling costs related to personalization and production of IDs.
- Matching security with functional requirements and choosing a technology appropriate for required levels of security.
- Designing back office systems that address security, card issuance, card and application life-cycle management, and data preparation and that incorporate appropriate standards (such as Global Platform, FIPS, and ISO/IEC).

One key decision is how to issue IDs. IDs can be issued centrally (all IDs are personalized or produced to some particular level in one location) or regionally through distributed workstations (two or more stations on site), or by using some combination of the two.

Issuing IDs centrally has the following advantages:

- Large volumes of cards can be personalized.
- Multiple constituencies are served quickly and securely.
- It is easier to adhere to the trust model.
- Management of card production and application loading is consistent.
- Control of production inventory (e.g., card stock, holograms) is easier.
- Enforcement of privacy procedures and application of standards is easier.
- Card printing, quality controls, and error rates are more easily tracked and managed.

Distributed issuance may be preferable when production volumes are smaller or where the cost benefits and efficiencies of central management don't have a large impact on the organization. Distributed issuance is also more appropriate when decisions about which applications to load on the ID are made locally or at the last minute, or in situations where immediate replacement of cards is mandatory (e.g., for physical access security or medical benefits). However, with distributed issuance, robust security procedures and adherence to strict process guidelines must be a high priority.

As for any investment decision, a cost benefit analysis should be performed to determine the ROI for each method.

Implementation Considerations for Managing ID Systems

All ID systems require management. At a minimum, the card database must be managed. A life-cycle management process is also required. A number of additional activities, such as developing the user interface to readers, training, and user support may also be necessary.

ID Card Management

Managing ID cards and the data on them is an integral part of any ID card system. A card management system must manage all data related to a card, such as the serial number and cardholder's personal information. Cardholder information is generally supplied by the card issuer, but may also

be supplied by the application owner. This data is saved in the card management database and is a key reference for any interaction with the cardholder or the card, such as for customer support, card re-issuance or card data changes.

Card security information includes specific keys and certificates that are used to initialize and personalize the card. This information is secure data and cannot be stored in the card management database unless it is needed for clearing a blocked card or installing additional data. This information must be stored in a secure format.

The card management system must also store appropriate application data. Application data include encryption keys, digital certificates, application names, version numbers, and dates of issuance. This information is needed to change the card or its applications, such as when a card is reissued or when new or updated applications need to be installed on the card.

In a smart ID card implementation, the system must also manage information about the chip. All card-specific information, such as operating system version, dates, unique card ID number, and keys and certificates that are used for enabling the card and its applications, must be managed. This information is needed for card personalization, for future changes to the card or its applications, and for re-issuing lost or stolen cards.

When a system involves cards that include multiple technologies (such as magnetic stripes and bar codes), the card management system must fulfill additional requirements, both for maintenance and integration of all technologies into the ID system.

ID Life-Cycle Management

Card life-cycle management functions are an integral part of any ID system. These functions can also be included in the card management system. Smart ID cards may require extra management because not only the card but also each application on the card must be managed.

Like other ID cards, a smart ID card that contains one or more applications goes through four stages during its lifetime: issuance, activation, deactivation, and reissuance. Each stage of the card's life cycle must be managed.

The applications loaded onto a smart ID card have life cycles similar to that of the card, although their life cycles may be independent of the card's physical life cycle. Applications can be issued with the card or at a later date. They can be blocked, restarted, and stopped at different times. Information about application life cycles must be managed.

Other Management Activities

Application life cycle information is typically managed by the issuing system (the host). Some card management actions, such as blocking a card, are also sent to the card from the host. To exchange data with the host, the card and the host must be able to communicate.

When cards include multiple applications, the relationship between the application providers and the card issuer needs to be managed. Typically, the applications loaded on a card each use a separate memory area and are distinct from other applications on the same card. However, some applications may need to interact with other applications. In this case, how these applications interact (on the card or on the host) must be managed.

In some situations, application providers are not application issuers. For example, a credit application may be designed by a bank card association, developed by a card manufacturer, and issued by the card-issuing financial institution. These relationships must also be managed by the card and application life-cycle management system.

Table 4 below summarizes key implementation considerations for issuing ID cards and managing ID systems.

Table 4: Example Implementation Checklist

Card Design	‣ Functional (name, demographics, photo) and aesthetic considerations ‣ Security features (overt, covert), as required
Card Type	‣ Smart card memory capacity ‣ Open or proprietary operating system ‣ Interoperability requirements
Applications	‣ Integration issues ‣ Local or central control ‣ Hardware requirements ‣ Partial or full initial implementation ‣ Migration strategy
Issuance	‣ Central or distributed issuance ‣ Initial card issuance strategy ‣ Remote issuance authority ‣ Replacements for lost/stolen cards ‣ Management of parallel systems during roll-out
Administration	‣ Business rules for card updates (e.g., changes in privileges, revocation, version control management) ‣ Business rules for adding, deleting or modifying applications ‣ Key management policies and procedures ‣ Business rules for system access and component administration ‣ Privacy policies ‣ Issuer and user training
Security and Audit	‣ Security procedures for card stock, issuance equipment and data access ‣ Audit procedures and controls for all issuance materials ‣ Security and audit procedures for system modifications and upgrades
Standards	‣ Compliance and how to enforce
Host/Back Office System	‣ Implementation of administration business rules ‣ Implementation of card and application life-cycle management ‣ Procedures and technologies for processing transactions received for authentication

Conclusions

Identification systems are needed by both public and private organizations. ID systems may operate completely within a single organization (an employee ID), span multiple organizations (across government bodies, between businesses and their customers), or extend out to the general population. Given the complexity of the identity verification problem, the number of involved parties, and the number of choices in ID system designs, it isn't surprising that many of today's ID systems are vulnerable.

To address these vulnerabilities and implement a secure ID system, organizations must define a chain of trust that encompasses all of the secure ID system processes and components. This chain of trust starts with the definition of a trust model, security policies, and business agreements among the organizations involved in the secure ID system and includes all of the components of the ID system – from the processes and documents that are used to initially verify an individual's identity and enroll that individual into the ID system to the usage of the system to the overall management of the ID system.

Smart cards are a vital link in the chain of trust for secure ID systems. They serve as the issuer's agent of trust and deliver unique capabilities to securely and accurately verify the identity of the cardholder, authenticate the ID credential, and serve the credential to the ID system. Smart cards are widely acknowledged as one of the most secure and reliable forms of electronic identification. As Table 5 shows, smart cards help address the issues and challenges that cause vulnerabilities in today's ID systems.

Table 5: Smart Cards and ID System Challenges

Issues & Challenges	How Smart Cards Help Address ID System Issues & Challenges
Inadequate security and privacy	• Smart cards strengthen the ID system's ability to protect individual privacy and secure personal information, providing authenticated and authorized information access, implementing a personal firewall for an individual and providing secure on-card storage of private information. • Smart cards provide strong ID card security. Smart cards are almost impossible to duplicate or forge, and data in the chip cannot be modified without proper authorization. • Smart cards increase the security and accuracy of identity authentication processes. • Smart cards used for logical access can store passwords, PINs and/or certificates securely and support single sign-on capabilities, improving enterprise logical security and simplifying identity management.
Identity not sufficiently verified	• Smart cards strengthen the security of identity authentication processes. • Smart cards provide a secure, convenient, and cost-effective technology that can store additional authentication factors (biometric, PIN, password, certificates) to more accurately verify that the cardholder is the individual authorized to hold the ID. • Smart cards provide strong ID card security, supporting features that deter counterfeiting and thwart tampering. • A single smart ID card used for logical access can store passwords, PINs, and/or certificates securely and support single sign-on capabilities.

Issues & Challenges	How Smart Cards Help Address ID System Issues & Challenges
Difficult credential management	• A single smart ID card can support multiple applications, simplifying the identification process for security staff, ID system administrators, and individuals. • The use of smart ID cards for logical access simplifies users' access to systems and provides for more straightforward management of logical access applications. • Information and applications stored on a smart card can be updated even after the card has been issued. This improves manageability and reduces the cost of an ID system, since new cards do not have to be issued to update data on the card or support new applications.
Multiple credentials	• A single smart ID card can support multiple applications, replacing multiple, hard-to-manage ID cards and implementing more straightforward logical access applications.
Proprietary and inflexible ID system	• Smart card technology is based on mature standards. Cards complying with these standards are developed commercially and have an established market presence. Multiple vendors are capable of supplying the standards-based components necessary to implement a smart card-based secure ID system, providing buyers with interoperable equipment and technology at a competitive cost.
Physical and logical convergence	• Smart cards support multiple applications, including both physical and logical access. Both contactless and contact smart card technologies can be used for access control applications.
Expensive to operate and support	• Multiple application smart cards can replace multiple separate ID cards, reducing overall cost and providing improved efficiencies in ID verification processes.
Usability problems	• Smart cards supporting multiple applications on single ID card provide improved user convenience. • Smart cards provide a convenient method for storing user information (e.g., password, biometric), making the authentication process easier and more convenient for the user.
Little or no apparent ROI	• The ability of smart cards to support multiple applications is a real advantage. The return on investment becomes more attractive when the ID system provides multiple benefits, either to multiple groups within an organization or across organizations. • A multiple technology smart card can ensure that a new ID system is interoperable with legacy systems and can provide a cost-effective migration path to new ID system technology.

As shown in this report, smart card-based ID systems offer significant benefits for individuals, businesses, and governments. Individuals using smart ID cards enjoy greater satisfaction through faster, more convenient and more secure access to information and services. The efficiency, consolidation of programs, and security features provided through the use of smart ID cards enable governments and businesses to enhance security while also improving services and reducing operating costs. Smart cards provide an optimal technology platform for a secure ID system that can meet government and business requirements for secure and accurate identification verification.

Reference and Resources

"Abstract of Concept of Operations for the Integration of Contactless Chip in the U.S. Passport," issued by the U.S. Department of State, Document Version 1.8. 17 September 2003

American Association of Motor Vehicle Administrators (AAMVA), www.aamva.org

Federated Electronic Government Coalition (FEGC). Additional information about how the federated identity trust model is being used can be found at http://www.fegc.org/pilotInfo.htm.

"Policy Issuance Regarding Smart Card Systems for Identification and Credentialing of Employees," Federal Identity and Credentialing Committee, February 2004, available at www.smartcard.gov/smartgov/information/scpfinal2004.doc

"Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology," Smart Card Alliance white paper, February 2003

Smart Card Alliance web site, www.smartcardalliance.org

"Smart Card Case Studies and Implementation Profiles," Smart Card Alliance report, December 2003

"Smart Cards and Biometrics in a Privacy-Sensitive Secure Personal Identification System," Smart Card Alliance report, May 2002

"Government Smart Card Handbook," U.S. General Services Administration, February 2004, available at www.smartcard.gov

"Using Smart Cards for Secure Physical Access," Smart Card Alliance report, July 2003

Publication Acknowledgements

This report was developed by the Smart Card Alliance to discuss the issues with current identification systems and to define the role that smart cards play in improving the accuracy, security and privacy of secure identification systems. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Secure Personal ID Task Force members for their contributions. Participants from 23 organizations were involved in the development of this report including: ActivCard, Alegra Technologies, AOS Hagenuk, ASSA ABLOY ITG, Atmel Corporation, Axalto, BearingPoint, Datakey, Datatrac Information Services, Inc., EDS, *e*ID Security, Gemplus, IBM, Identix, Infineon Technologies, LaserCard Systems, Lockheed Martin, MartSoft Corporation, Northrop Grumman Information Technology, Philips Semiconductors, Smart Commerce, Inc., Unisys, U.S. General Services Administration.

Special thanks go to the individuals who wrote, reviewed and edited this report.

David Asay, IBM
Ralph Billeri, BearingPoint
Iana Bohmer, Northrop Grumman Information Technology
Kirk Brafford, ActivCard
Yuh-Ning Chen, Ph.D., MartSoft Corporation
Patrice Erickson, Identix
John Harrison, IBM
Mansour Karimzadeh, Smart Commerce, Inc,
Colleen Kulhanek, Datakey
Vince Ley, Datatrac Information Services, Inc.
Jeff Katz, Atmel Corporation
Mark McGovern, Lockheed Martin
John McKeon, IBM
Cathy Medich, Consultant and Task Force Chair
Bob Merkert, SCM Microsystems
Neville Pattinson, Axalto
Dwayne Pfeiffer, Northrop Grumman Information Technology
Tate Preston, *e*ID Security
Bob Wilberger, Northrop Grumman Information Technology

Copyright Notice

Trademark Notice

Appendix A: Organization Profiles

Many organizations in the U.S. are working on improving the security and accuracy of identification systems. This appendix includes brief profiles of a number of organizations who are either implementing new secure ID systems or who are developing the trust models and policies that other organization can use to improve ID systems.[5]

- American Association of Motor Vehicle Administrators (AAMVA) – Driver License/ID Security Framework
- U.S. Department of Defense Common Access Card
- Federated Identity and Cross-credentialing System (FiXs)/Defense Cross-credentialing Identification System (DCIS) Proof of Concept
- Transportation Security Administration Transportation Workers Identification Credential (TWIC)
- U.S. Department of State: Concept of Operations for the Integration of Contactless Chip in the U.S. Passport
- Rabobank

American Association of Motor Vehicle Administrators – Driver License/ID Security Framework[6]

In 2001, AAMVA formed a Special Task Force on Identification Security with members from U.S. and Canadian AAMVA jurisdictions. The Task Force was organized into five working groups focusing on technology, new issuance/initial identification, residency issues, document security standards, and communications/advocacy. AAMVA subsequently set up 14 Task Groups to research and report on critical issues. Working across federal, state and provincial government agencies and with support from a wide range of industry resources, a comprehensive range of decisions and recommendations have been developed or are still under consideration.

The security framework acknowledges that development and ongoing maintenance of a secure ID program requires a broad approach with minimum standards adopted and adhered to in order to promote ID security, interoperability, and jurisdictional reciprocity. Five critical areas were identified in this effort:

- Business requirements. This area includes internal controls, policies, procedures, staff training, and technology that must first be in place as the internal components for any organization that issues a secure document.

[5] Additional user profiles can be found in the Smart Card Alliance report, "Smart Card Case Studies and Implementation Profiles," available at www.smartcardalliance.org.

[6] For a complete review of the AAMVA Special Task Force on Identification Security, visit the AAMVA website at: http://www.aamva.org/idsecurity/idsExecutiveSummary.asp

- System and business integrity. This area includes the rules and practices that assure compliance with the established business requirements, such as audit and security plans as well as oversight rules.
- Initial customer identification. This area details how to positively identify a customer. It includes the use of acceptable verifiable resource lists (proof documents), procedures for using the lists, verification of information (electronically), and customer notification of rights and responsibilities concerning the use of personal information and privacy.
- Record and document creation. This area includes the collection of personal data, the driver's license/ID card design specifications, unique identifiers for individuals, automated record creation and maintenance, and card production security and techniques for issuing systems. AAMVA has already issued a specification for a common format for the driver's license/ID card covering data elements, layout and security.
- Record and document use. This area includes the management and use of both electronic records and physical documents by administrators, law enforcement, other government agencies, businesses and other private users. Penalties and sanctions, as well as information use restrictions, are included in the form of model legislation.

Significant efforts were directed at defining the process for establishing an applicant's identity. Fraudulent document recognition training courses were developed and are being rolled out across all AAMVA jurisdictions. As part of that process, standards were also set that establish a list of documents that can be used to establish identity, and recommendations were made about processes for verifying those documents. In addition, a new specification was developed that defines requirements for the driver's license/ID card design.

AAMVA's work continued with the publication of best practices or recommended guidelines for internal security and audit, and with model legislation covering offenses and penalties. AAMVA announced that collection of biometrics for the enrollment verification process was considered; however, AAMVA concluded that the technology could not currently support a database of 300 million individuals for identification, and deferred any recommendation on biometrics.

U.S. Department of Defense Common Access Card[7]

One of the most advanced smart ID card programs in the U.S. is the U.S. Department of Defense (DoD) Common Access Card (CAC), a smart card that will serve as the DoD standard identification and physical access credential as turnstiles are installed for machine-readable authentication and access at DoD facilities over the coming years. The card is currently used for secure authentication and network access. The card is issued to active duty military, selected reservists and National Guard, DoD civilian employees and selected DoD contractors. As of January 2004, DoD had issued 4.4 million smart cards, with issuance expected to be complete by Spring 2004. The population receiving cards includes all active military and reserves, their contractors and visitors. DoD has deployed an issuance infrastructure in over 900 sites in more than 15 countries around the world, and is rolling out more than 1 million card readers and the associated middleware. A key goal

[7] Additional information about the DoD CAC program and other U.S. government smart card initiatives can be found at http://www.smart.gov/smartgov/smart_card.cfm.

of the CAC program is to meet DoD's mandate to digitally sign all electronic mail and other electronic documents.

Future plans include: using the CAC for signing and encrypting email; expanding the number of portals capable of doing web-based e-business using PKI authentication tools; adding a biometric to the cards to provide three-factor authentication; and expanding the use of the cards for physical access by adding a contactless chip when approved, using ISO/IEC 14443 Parts 1-4 with a FIPS-approved algorithm.

DoD is developing a comprehensive identity protection program that provides strong authentication for identity credentials at the front-end, secure smart card credentials and strong identity binding to the back-end system using biometrics. DoD is working with industry on the Federated Identity Cross-credentialing System (FiXs)/Defense Cross-credential Identification System (DCIS) proof of concept project. This project implements an identity management and credentialing system between DoD and industry participants that have a need for employee identification and authentication as part of their joint working environment. An initiative is being pursued under the Federated Identity Cross-credentialing System to extend the cross-credentialing efforts to Federal agencies outside of DoD.

As the CAC identity credential is now in the final stages of issuance to all active military, DoD is beginning to concentrate on incorporating the CAC into many other applications as they are renewed, to exploit the benefits of machine-readability into other DoD applications.

DoD is also in the early stages of planning to serve other large communities that are closely tied to Defense, including the DoD military dependents, DoD recipients of health care services from the Tri-Care medical system, and veterans.

Federated Identity and Cross-credentialing System (FiXs)/Defense Cross-credentialing Identification System (DCIS) Proof of Concept[8]

The Department of Defense and a coalition of private-industry partners have launched a proof of concept and pilot project to demonstrate the interoperability of credentials for physical access to work locations. (A follow-on phase will deal with network access.) The Federated Identity and Cross-credentialing System (FiXs)/Defense Cross-credentialing Identification System (DCIS) will implement an identity management and credentialing system between DoD and industry participants that need employee identification and authentication as part of their joint working environment.

The FiXs/DCIS project is being conducted under the auspices of the Federated Electronic Government Coalition (FEGC). The Defense Manpower Data Center (DMDC) is the federal sponsor of the project, and the following companies are participating in the initial phase, which runs from October 1, 2003 through August 31, 2004:

- BearingPoint, Inc.
- Electronic Data Systems, Inc.
- Northrop Grumman
- SRA International, Inc.
- Anteon
- Lockheed Martin

[8] Additional information can be found on the Federated Electronic Government Coalition (FEGC) website at http://www.fegc.org/pilotInfo.htm.

The FiXs/DCIS project will enable participating DoD facilities to achieve strong authentication of participating contractor personnel who present a company-issued trusted credential. Similarly, participating locations will also recognize a DoD-issued Common Access Card. At the same time, the FiXs/DCIS program will permit DoD and its contractors to maintain existing security systems and policies.

The key to the success of FiXs/DCIS is interoperability. Interoperability is achieved via a common trust exchange policy, operating rules and technical specifications that allow various parties to act and exchange information on an equal basis. FiXs/DCIS borrows many of its concepts from the electronic payments industry. In the electronic payments industry, specific operating rules provide a uniform business and legal framework, as well as standard formats, for the exchange of financial payments. To rely on the principles already established for the payments industry, NACHA – The Electronic Payments Association assisted with its knowledge and experience in developing the FiXs/DCIS operating rules. Since processing an employee's credentials is analogous to processing a payment, operating rules for cross-credentialing will also permit maximum participation among various parties that would otherwise use differing practices and platforms. The goal of the project is to establish a "chain of trust" for contractors, delivery and repair personnel, and employees of other government agencies, who require frequent access to DoD and industry facilities.

When participants enroll in the program, their identities are verified using several forms of identification, and biometrics are captured. When participants present themselves at a FiXs/DCIS-enabled facility, their identity can be authenticated. All local DoD and industry physical access control procedures apply.

The Phase-I proof of concept and pilot will be implemented at select DoD and participating industry facilities in: Alexandria, McLean and Reston, Virginia; Columbia, Maryland; Wright-Patterson Air Force Base, Ohio; Kirtland Air Force Base, New Mexico; and DMDC West, Defense Language Institute and the Naval Post Graduate School, Monterey, California.

Following completion of the first phase, FEGC officials anticipate that additional federal agencies and industry representatives will participate in the project. In Phase-II, DoD is looking to extend the solution to control network access with its industry partners.

Transportation Security Administration Transportation Workers Identification Credential (TWIC)[9]

The Transportation Security Administration (TSA) is mandated by federal legislation to develop an identification system for individuals requiring access to secure areas of the nation's transportation system. The Transportation Worker Identification Credential (TWIC) is intended for each worker requiring unescorted physical or logical access to secure areas of the nation's transportation modes (maritime, aviation, transit, rail, and other surface modes).

The TWIC will allow implementation of a nationwide standard for secure identification of transportation workers and access control for transportation facilities. Current estimates are that 12 to 15 million workers will require the

[9] For additional information, see TWIC Stakeholder Brief at http://www.tsa.gov/public/interweb/assetlibrary/TWICbrief25dec.pdf

TWIC to gain access to secure transportation sites. Each individual enrolled in the TWIC system will be positively matched to his or her credential via a reference biometric (or multiple biometrics) and will have undergone a standard background check.

The program infrastructure carefully balances security, commerce, and privacy requirements. The TWIC threat mitigation goals are to:

- Uniformly and consistently ascertain identities.
- Uniformly and consistently match an individual to a valid credential and background check.
- Uniformly and consistently conduct access threat assessment.
- Provide a tamper-resistant credential.

The TWIC is to be universally recognized so that workers will not require redundant credentials or background investigations to enter multiple secured work sites and will allow facilities to better manage site access. Additionally, the credential will have the capability to be used within a facility to meet multiple levels of secure access requirements.

The TWIC system will contain sufficient technologies to be compatible with the Government Smart Card Interoperability Specification (GSC-IS) while maintaining access to and within local facilities. This will enable the TWIC to leverage existing access control system investments, rather than require replacement of these systems at considerable expense. Additionally, the TWIC system will serve as the standard platform for future technology purchases at transportation facilities.

The TWIC program conducted two regional multi-modal pilot projects. The Los Angeles/Long Beach and Philadelphia/Delaware River areas were the TWIC regional pilot sites based on the broad range of facility types (e.g., mode, size, infrastructure), organization structures, transportation mode inter-relationships, and policy issues in each region.

TSA completed a technology evaluation in late 2003 and determined that smart card technology is the most appropriate technology for TWIC's requirements, providing a commercially available, secure solution for both physical and logical access. TWIC program personnel is now planning a seven-month prototype phase which will begin in early 2004 and will introduce biometric identifiers and contactless technology. The prototype phase will include both pilot regions and add Florida airports and seaports.

United States Passport: Concept of Operations for the Integration of Contactless Chip[10]

The Department of State, Bureau of Consular Affairs, in cooperation with its partners at the United States Government Printing Office and the Department of Homeland Security, plans to implement a new version of the United States passport that will contain an embedded contactless integrated circuit (IC) chip. The chip will be used to store additional data on the passport that cannot be stored in the conventional OCR-B machine readable zone. The new technology will enhance the security of the passport and will facilitate the movement of travelers at ports of entry. The new passport initially will be

[10] This profile is extracted from, "Abstract of Concept of Operations for the Integration of Contactless Chip in the U.S. Passport," issued by the U.S. Department of State, from Document Version 1.8, 17 September 2003.

issued on a limited scale by October 2004. All newly-issued, full-validity United States passports will have embedded chips by the end of calendar year 2005.

Background

Section 303 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Enhanced Border Security Act) requires that nations whose citizens are allowed to enter the U.S. under the provisions of the Visa Waiver Program (VWP) must have a program in place by October 26, 2004 to "incorporate biometric and document authentication identifiers that comply with applicable biometric and document identification standards established by the International Civil Aviation Organization (ICAO)."

ICAO, through a series of meetings during the last year, has developed a set of specifications that involve the inclusion of an electronic chip in passports to which would be written both the facial image and biographic data of the bearer. This is the same data currently found on the data page of a passport.

Including an IC chip in passports could provide the border inspection community with a tool that can have significant security benefits and could speed the movement of travelers through border inspection processes.

While the United States is not mandated to comply with the requirements of section 303 of the Enhanced Border Security Act, it appears desirable for the U.S. to commit to a comprehensive program to incorporate this new technology into the U.S. passport. Doing so will:

- Ensure the continued international acceptability and interoperability of U.S. passports.
- Recognize that VWP participant states, which will be required to change their passports for travel by their nationals to the U.S., will be likely to impose reciprocal requirements on Americans traveling to their nations.
- Improve the security of the U.S. passport and help strengthen U.S. border security by allowing the Department of Homeland Security to focus its efforts on travelers (American and otherwise) with less secure travel documents.

Consistent with principles of international reciprocity, the United States intends to adhere to these same requirements. Therefore, the United States intelligent passport will be designed to comply with the specifications of the ICAO, Document 9303, Part I and its technical reports and annexes relating to advanced storage media for use in passports. As such, the passport will include a full digital image of the passport bearer stored on an IC chip and will incorporate the use of the ICAO Logical Data Structure which prescribes the placement of data on the chip. The data stored on the chip will be secured with a digital signature using a light version of public key infrastructure (PKI) technology as prescribed by ICAO.

The Under-Secretary of State for Management has authorized Consular Affairs (CA) to pursue the concept of integrating a contactless chip in the United States passport and to comply with ICAO requirements regarding the use of this advanced storage medium to store a digital, biometric full facial image along with currently captured biographic data onboard the chip.

Rabobank[11]

With 33,000 of its 50,000 worldwide employees serving 9 million customers in the Netherlands, Rabobank Group is the largest Dutch retail bank, operating nearly 1500 offices and 380 local banks. Rabobank Group's specialized banking businesses are market leaders in virtually all financial services – from leasing and trade finance to insurance, venture capital and private banking

Customer demands for trust and security have remained constant while revolutionary changes in banking practices and technologies over the past century have completely changed the culture of the industry. An increasing number of technology-savvy financial customers around the world expect to initiate secure transactions via the Internet or by phone anytime, anywhere. As a result, large financial organizations such as Rabobank Group have put security strategies in place, both internally and externally, to keep pace with the technology requirements of electronic banking.

Rabobank Group has stayed several steps ahead of these increasingly complex technology challenges by consistently investing in a security infrastructure and strategy it calls Rabo Web Security (RWB), deployed enterprise-wide by its Zeist-based ICT Group.

"The bank's way of working today is quite different from the past and much more distributed," says Ad Bezemer, Project Manager of Infra Services at Rabobank ICT headquarters in Zeist. "Financial services have become much more complicated, as integrated products and several distribution channels are emerging. In the past, security meant shielding off hackers and intruders, but today, it means building the highest levels of trust right into our systems and communications."

To build the highest levels of trust into its systems as it moves closer toward the future vision of "anytime, anywhere banking," Rabobank ICT has applied its forward-looking security strategy on several fronts, including its internal communications and channels. Since 1997, Rabobank ICT has been moving all applications, which in the past had disparate security and required multiple passwords, to the intranet in order to make them available on all distribution channels. "This move enables us to centralize the security around these applications," explains Ad Bezemer.

To control access to these centralized applications and ensure strong authentication of its internal bank employees, Rabobank is deploying 33,000 smart cards combined with PKI (public key infrastructure) technology that enable a new level of security and efficiency for its internal employees.

At Rabobank, the deployment of smart cards is eliminating the risks inherent in a "knowledge only" system based on multiple passwords. This is accomplished by using two-factor security – *something that is owned* (the smart card) and *something that is known* (the user's password). In e-business security language, the smart cards provide non-repudiation – two-factor security authenticates unequivocally that users truly are who they claim to be – and therefore integrity and security

Because Rabobank's cooperative banks decide independently on their local needs and requirements, some are using the smart cards for physical

[11] For additional information, a full case study is available in the Smart Card Alliance report, "Smart Card Case Studies and Implementation Profiles," available at www.smartcardalliance.org .

access. To meet the specific requirements of those banks, the smart cards are delivered custom-formatted with magnetic stripes and proximity technology. Whatever type of smart card the individual banks prefer, employee uses include network access, Microsoft Windows™ logon, and digital signatures.

Rabobank has given several hundred additional smart cards to large customers for special transactions. In international scenarios, for example, the smart card is used for dealing room currency transactions. The customer is able to do an immediate buy or sell in the exact dollar (or other currency) amount without incurring the risk of losing funds through currency fluctuations. "By ordering the currency transaction directly with the smart card, the customer is able to side-step the process of calling the bank and arranging a transaction which may take a month or two to complete," says Ad Bezemer. "The usually 10-second confirmation makes the transaction almost real-time, versus the risky delays with the old process. The smart card offers our currency-trading international customers speed, cost-efficiency and transactional security.