Personal Identity Verification System: Identity Verification Cards

NOTE: This document is based on a publication of the Smartcard Alliance (see Acknowledgements on page 24). It is provided as background information and is not a recommendation of NIST.

Introduction

Security is one of the most demanding requirements in our modern society. Security includes personal safety, personal information protection, personal and organizational asset protection, and physical control of access to facilities and localities. Security always starts with a policy that states who is responsible for protecting "what" for "whom" against "which" threat. The "what" can be a tangible asset, such as a physical object, or an intangible asset, such as information, rights, or privileges. In all cases, assets have significant value to the "whom." Identifying the "whom" properly is the first requirement of a security program. Identifying the threats and their resulting risk are the objectives of a risk analysis which must be done before initiating implementation of a PIV system.

Virtually every source of threats and method of 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 an object and then allow them access that has been specifically authorized. Everyone else should be rejected. Such identification capabilities are carried out by a secure personal identity verification (PIV) system.

Essential to a secure ID system is the concept of "*trust*." Trust in procedures, automated processes, people, the security architecture and selected technologies is vital to building and having confidence in a secure PIV system. A chain of trust is a linkage of the sequence of steps in a secure system starting with the "naming" of a person at birth through each and every decision to grant or deny access to the individual claiming to be that person. A secure PIV system "guarantees" (to some level of assurance implicitly or explicitly stated) the authenticity of the people, identity credentials, identity token issuing organizations, token reading/writing devices, data processing equipment, communication networks, and other components of the automated system. The chain of trust must also ensure that information entered into and used within the system is verified, authenticated, protected and used appropriately.

This PIV standard establishes a framework of the elements that are essential to creating and maintaining a secure PIV system and its appropriate "chains of trust:"

- The trust model adopted within an organization or among organizations that participate in a PIV system
- The procedures used to verify that people are who they claim to be and then enroll them in the PIV system
- The process that verifies claimed identities and validates 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 can provide a vital link in a chain of trust. They can be used within a Personal Identity Verification system to 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 standard establishes the framework and its underlying components that comprise a secure PIV system. It specifies personal enrollment, Personal Identity Credential (PIC) creation and issuance in an electronic token, identity verification, access authorization, and access approval processes. This standard specifies use of an identity token as a major component and specifies the requirements of smart cards in the chain of trust of a secure PIV system.

How Today’s Identification Systems Can Fail

A person has only one “identity” but may have identifiers (e.g., birth name, religious name, SSN, military ID number) and may carry multiple identification cards or tokens that are issued by multiple public and private organizations. Such tokens include driver’s licenses, membership cards, credit cards, and corporate identification badges.

The primary purpose of an ID token is to verify that the holder has particular rights, privileges, and responsibilities within some context or environment. ID tokens may verify a person’s identity and specify authorization to perform some activity (for example, a driver’s license verifies the license-holder’s right to operate a motor vehicle). Historically, certain tokens, such as a driver’s license, are also used by organizations that do not issue their own tokens.

Systems that issue ID tokens are typically one of two types:

- Systems that interface with members of the public, such as a driver’s license system, health entitlement system, or passport system. Such systems are *open systems*.
- Systems that interface with closed groups such as government employees and issue employee badges. Such systems are closed *systems*.

Many of today’s identification systems are vulnerable. They often use tamper-prone credential carriers 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.

Table 1: ID System Issues and Challenges

Issues and Challenges	Open Systems	Closed Systems
Many of today’s ID verification systems fail to provide adequate security and privacy	• Recent terrorist attacks point out the need for better identity systems. • Identity theft has become a major problem in entitlement systems. • Cyber-terrorism is an emerging threat.	• Most government agencies perform their own identity “proofing” of prospective employees and issue their own ID badges • Agencies rarely accept ID badges from other agencies as adequate for access
Proving the “true” identity of a person seeking an identity	• Legitimate persons can have unreliable or missing identity documentation. • Persons can easily obtain counterfeit or	• Employers encounter job applicants who misrepresent their identities when seeking employment.

Issues and Challenges	Open Systems	Closed Systems
credential token can be difficult	fraudulent identity source documents. - Identity theft often starts with a thief using genuine identity source documents to get a legitimate identity token.	
Identity is not sufficiently verified in most ID systems today	- Many 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. - Identity verification is often based on the observations and discretion of the person or official checking the ID.	- 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.
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	- Governments often require their own IDs for foreigners within their borders. - 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 other agency's 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 closed PIV systems require management of 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	- Open systems have traditionally used identity tokens only for PIV for facility access. 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	- Users must often apply for new or duplicate IDs when moving to a new	- Users must juggle too many IDs on a daily basis.

Issues and Challenges	Open Systems	Closed Systems
usability problems	jurisdiction. • Users must often deal with long wait times and poor customer support.	• Most of today’s ID systems fail to alleviate administrative overhead, consolidate user credentials, and close security holes.

What Makes an Identity Verification System Secure

A secure PIV system is designed to accomplish one primary goal: verify that an individual is who the individual claims to be. When properly designed, secure PIV systems implement a chain of trust, assuring everyone involved that the individual presenting an ID token is the person who owns the credentials on the token and that the credentials are valid. (The term "credential" refers to information stored on the card that represents the individual's identity and access privileges.) A secure PIV 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 information system is a secure PIV token (i.e, badge, electronic device, smart card) and often called an ID card. The PIV token (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 PIV system must assure that a legitimate authority issued the token, that the token and the credential it carries are not counterfeit or altered, and that the person carrying the token matches the individual who enrolled in the PIV system.

The use of smart ID devices, especially in the form of smart cards, offers advantages for both physical and logical security. Smart identity verification tokens 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 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 Secure PIV System Trust Model

Secure PIV 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, PIV 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 a PIV system must define and agree to a trust model.

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

The *federated identity trust model* 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 PIV system operating rules and business procedures and is especially relevant for systems that involve multiple, independent organizations.

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 identity 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 “prove” or verify a person’s identity prior to issuance of a credential

2) Verifying identities whenever individuals present themselves to the PIV system

Design Elements that Make a PIV System Secure

Secure PIV system design requires a set of decisions that select and implement policies, procedures, architecture and technology. 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 PIV token.

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

- A secure enrollment process that establishes (i.e., “proves” to some level of assurance) an individual’s identity and, in cases that a PIV token is also used for access authorization, determines that the person is entitled to the privileges that are being granted
- Procedures for securely issuing PIV cards and ensuring that PIV tokens are issued only by authorized issuing organizations and only to the correct person
- Policies and procedures for monitoring the use of the PIV
- Procedures for PIV life-cycle management
- Training for users and issuers
- Policies, procedures and technologies that protect access to the information in the system about PIV holders

- Security controls that provide only authorized viewers with access to information on the PIV
- An authentication process that implements the defined chain of trust, verifying the identity of PIV holders and the legitimacy of the PIV cards and their credentials

Components of a Secure PIV System

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

Table 2: Secure PIV System Components

Component	Key Design Decision
Trusted Issuing Authority	‣ What trust model organizations participating in the PIV 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 PIV personalization process should be ‣ How to be sure the distribution process complies with the defined security policy ‣ How to implement PIV inventory physical security ‣ How to audit PIV cards ‣ How to implement data security ‣ What the life-cycle management process should be
PIV Credential / Card	‣ What types of applications to support, now and in the future ‣ What the PIV 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 PIV should be used and under what conditions ‣ The type of PIV 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

Component	Key Design Decision
	‣ Under what conditions to use biometrics
PIV Readers	‣ Location, number, and architecture of PIV readers and how to protect them ‣ Design and appearance of the readers ‣ How the PIV 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 PIV Systems

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

To be considered "privacy-enabled," a PIV 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

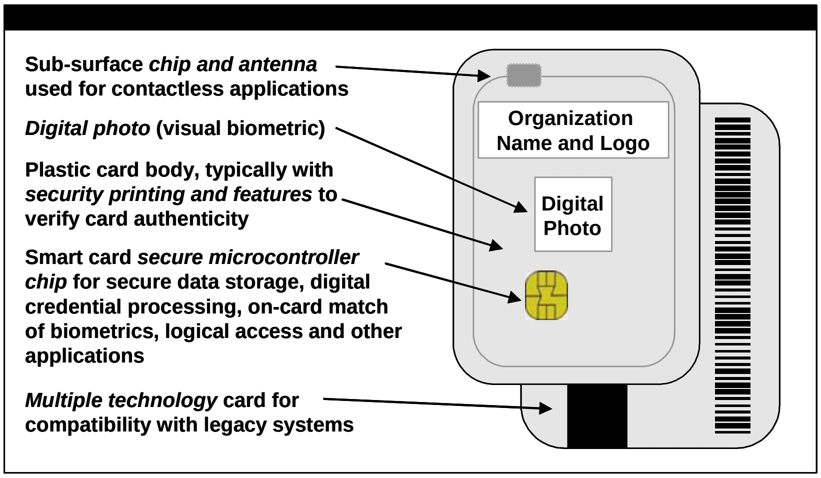
A number of government organizations and industry groups have developed recommendations for fair information practices and guidelines to protect individual privacy. System designers need to consider business practices, security policies, and system architectures, as well as technologies, in developing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

Smart Cards and Secure PIV Systems

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

Figure 1: PIV Smart Card Example



Sub-surface *chip and antenna* used for contactless applications

Digital photo (visual biometric)

Plastic card body, typically with *security printing and features* to verify card authenticity

Smart card *secure microcontroller chip* for secure data storage, digital credential processing, on-card match of biometrics, logical access and other applications

Multiple technology card for compatibility with legacy systems

Secure Identification System Enrollment

A critical link in the chain of trust for a secure PIV 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 PIV 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 PIV 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 PIV system to verify identity.

The Enrollment Process

A secure enrollment (i.e., identity registration) process must be well planned to avoid fraud and to make the process as seamless as possible. Enrollers (i.e., registry authorities, registration agents) need to be trained and educated to understand their roles, the characteristics and functions of the PIV card, and the importance of enrollment. Enrollees (i.e., identity registration applicants) must prove their identity to the enroller. Enrollee information should be checked by the enroller to ensure that the person has not already enrolled as someone else, possibly with different demographic data. This last objective is very difficult to achieve in a large, distributed identity register since it involves comparing identity source information (e.g., fingerprints, handwriting characteristics) against the entire existing identity register looking for duplication.

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). PIV holders must be educated during the enrollment process, not only on enrollment but also on the use of the PIV. Lastly, the process must ensure the PIV 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 identity "proofing", independent identity register database checks).

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 an original identity establishing document (e.g., birth certificate) that can be used to create subsequent identity verification documents.

Depending on the PIV system enrollment process, a breeder document can be a birth certificate or an equivalent foreign identity establishing document. Identity credentials that are derived from a breeder document should contain a "chain of trust" back to the breeder document for later verification. A derived identity credential token may be used as a breeder document to obtain other identity credentials if and only if this "chain of trust" is verified by the enroller and contained on the new identity token.

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

PIV System Use of Biometrics

New secure PIV system implementations are requiring one or more biometrics to provide increased assurance that an individual presenting the PIV card has the right to use that PIV. Biometrics are defined as automated methods of verifying 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:

- DNA, based on the differences among the genetic characteristics of people
- 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
- Signature, based on the speed, stroke order, and pressure derived from a written pattern
- Voice, based on spoken phrases
- Retinal, based on patterns on the rear of the eye

Printed biometric information, such as photographs, height, weight, eye color, and hair color, has been used for years to verify a claimed identity. These biometrics are verified visually by another person. However, visual verification is a subjective process, and the inspector sometimes can be fooled by clever, competent, and motivated impersonators. In addition, an enrollee may not provide accurate information originally (e.g., incorrect weight, wrong eye color) or the PIV token holder's appearance may have changed since enrollment.

Issues with Enrollment and PIV Token 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 PIV token and associated technologies, which are likely to be new to the PIV token holder. Where appropriate, educating the user about how and where biometric templates are stored and used can ease concerns about privacy. For example, a smart card is used in some PIV systems, with biometric templates stored exclusively on the card and accessed only if the user presents the card to an authorized system. PIV 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 identity verification 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, identity verification by an operator is possible.

When enrollment is implemented electronically, an enrollee’s PIV 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 be delivered to the cardholder securely.

Regardless of where an PIV 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 PIV tokens is also an issue. An appropriate PIV system can “hot-list” tokens reported as missing and issue a replacement without requiring reenrollment. When a hot-listed token is read by a device that is hot-list enabled, the token can be disabled, confiscated, or ignored, as appropriate.

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

The chain of trust for a secure PIV 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 PIV credential once the PIV token has been issued and is in use. To illustrate the strongest possible chain of trust, the discussion assumes that the PIV 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 a PIV token in a secure PIV system assures the following:

- The PIV token holder is the person enrolled in the PIV system with that claimed identity and is the valid user of the PIV token.
- The PIV token holder has authorized the release or use of the PIV credential for identity verification.
- The PIV credential presented is valid (i.e., genuine, unaltered and not expired) and is from the authorized issuer.
- The PIV token (e.g., passport or smart PIV card) is valid, is not counterfeit and is appropriate for the PIV credential being carried.
- The electronic device and the data stored therein contained in the PIV token is valid and not counterfeit.
- The external device reading the PIV is an authentic, authorized part of the PIV system and is trusted to perform specific identity verification tasks.

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

Physical PIV Verification

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

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

In all cases, the PIV token 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)

PIV Device Authentication

To ensure that the electronic device used on the PIV 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 PIV token. The authentication process may be accomplished between the token 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 a token using a symmetric shared secret key, both the PIV 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 PIV device to the reader and verified against an independent calculation performed by the challenger. If the results match, the PIV token 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 PIV 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 PIC, 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 PIV token 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 PIV. In this case, the PIV would issue a challenge to the reader and verify the result with an internally calculated value. Without a satisfactory response, the PIV 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 PIV tokens.

PIV Credential Authentication

The digital credentials stored on the PIV 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.

PIV Holder Authentication

The identity of a person holding a PIV token can be verified in two ways, by checking:

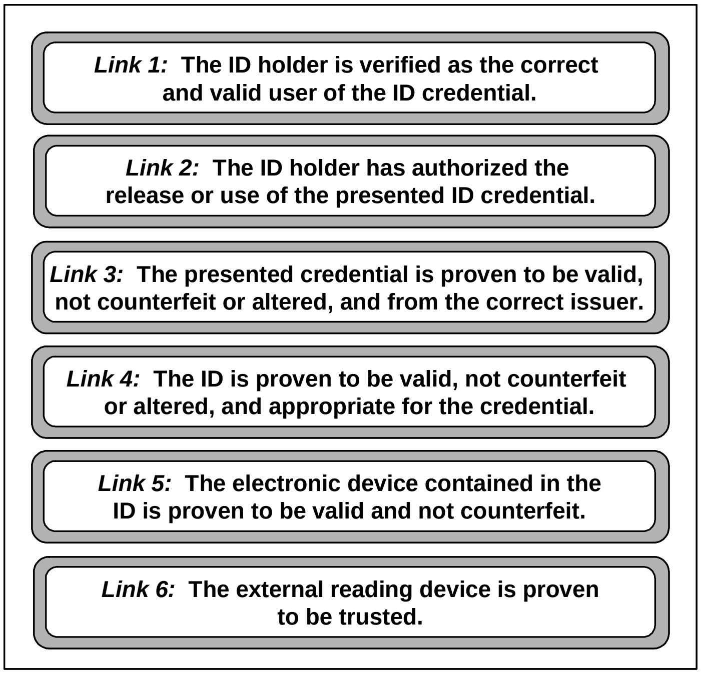
- What the user knows (for example, a PIN or password), and/or
- What the user is (for example, a biometric).

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

To check "what the user is," either the photo on the PIV card is compared to the face of the presenting PIV holder or an automated biometric match is done. Biometric-based PIV 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 PIV holder is the same person who enrolled in the PIV system and is the correct person to use the PIV. Biometrics can also protect access to the credentials on an PIV.

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

Figure 2: The Chain of Trust during PIV Usage



***Link 1:* The ID holder is verified as the correct and valid user of the ID credential.**

***Link 2:* The ID holder has authorized the release or use of the presented ID credential.**

***Link 3:* The presented credential is proven to be valid, not counterfeit or altered, and from the correct issuer.**

***Link 4:* The ID is proven to be valid, not counterfeit or altered, and appropriate for the credential.**

***Link 5:* The electronic device contained in the ID is proven to be valid and not counterfeit.**

***Link 6:* The external reading device is proven to be trusted.**

The Role of Smart Cards in the Chain of Trust

Smart card technology strengthens many of the links in the chain of trust in a secure PIV system. Smart cards can act as the individual's PIV card and allow secure access to facilities, 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 human and electronic identity verification in both the physical and digital worlds. This can generate significant savings as the smart card-based PIV 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 identity relevant information is the individual's age. Whether the individual can drive and where the individual lives are irrelevant.

The smart card's ability to process information and react to an 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 identity tokens (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 PIV Card Security. When compared with other tamper-resistant PIV cards, smart cards represent a 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 PIV cards will also be used for manual identity verification, visual security features can be added to a smart card body.

PIV Credential Security. Protecting the privacy, authenticity, and integrity of the data encoded on a PIV card as credentials is a primary requirement for a secure PIV system. Sensitive data is typically encrypted, both on the smart PIV 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 PIV system may require that system components authenticate the legitimacy of other components during the identity verification process. The smart PIV card can verify that the card reader is authentic, and the card reader in turn can authenticate the smart PIV card. The smart PIV 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. Unlike other identity verification 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 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 PIV system can protect an individual's privacy while ensuring that the individual is properly identified.

Smart Cards and Biometrics. Secure PIV 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 PIV 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 PIV 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 PIV 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 PIV card and credential is mandatory for a secure PIV system. With the advent of smart cards, electronic devices that store PIV 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 PIV card) is the portable digital security agent of the issuer and is a vital link in the chain of trust for any serious secure PIV system.

Implementation Considerations for Smart Card-Based Secure Identity Verification Systems

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 sense.

The amount of effort that an organization makes in using 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. Another factor to consider is the potential impact of legislation and policy on the environment in which the organization operates. For example, there is now an enormous push to improve “cybersecurity,” 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.

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 PIV program that supports strong authentication and single sign-on applications.

The institution of a smart card-based secure PIV 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. 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 PIV 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.

Table 3: Example Applications for a Multi-Application Smart PIV 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 PIV Cards

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

- Collecting and handling all card data securely.
- Managing the storage of card data securely and with attention to privacy issues.
- Delivering ID tokens to end users promptly and efficiently.
- Controlling costs related to personalization and production of tokens.
- 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.

One key decision is how to issue tokens. Tokens can be issued centrally (all tokens produced in one location) or regionally through a distributed process. Issuing IDs centrally has the following advantages:

- Large volumes of cards can be quickly created.
- It is easier to adhere to one 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 needed where the organization itself is geographically distributed or the cost benefits and efficiencies of central management are negligible. Distributed issuance is also more appropriate when decisions about which applications to load on the PIV 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.

Implementation Considerations for Managing PIV Systems

All PIV 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.

PIV Card Management

Managing PIV cards and the data on them is an integral part of any PIV 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 PIV card implementation, the system must also manage information about the chip. All card-specific information, such as operating system version, dates, unique card PIV 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 PIV system.

PIV system Life-Cycle Management

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

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

The applications loaded onto a smart PIV 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 PIV cards and managing PIV 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	• Rules for card updates (e.g., changes in privileges, revocation, version control management) • Rules for adding, deleting or modifying applications • Key management policies and procedures • 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 rules • Implementation of card and application life-cycle management • Procedures and technologies for processing transactions received for authentication

Conclusions

Identity verification systems are needed by government organizations. PIV systems may operate completely within a single organization (an employee PIV) or span multiple organizations (across government bodies),. Given the complexity of the identity verification problem, the number of involved parties, and the number of choices in PIV system designs, it isn't surprising that many of today's PIV systems are vulnerable.

To address these vulnerabilities and implement a secure PIV system, organizations must define a chain of trust that encompasses all of the secure PIV 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 PIV system and includes all of the components of the PIV system – from the processes and documents that are used to initially verify an individual's identity and enroll that individual into the PIV system to the usage of the system to the overall management of the PIV system.

Smart cards are a vital link in the chain of trust for secure PIV 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 PIV credential, and serve the credential to the PIV system. As Table 5 shows, smart cards help address the issues and challenges that cause vulnerabilities in today's PIV systems.

Table 5: Smart Cards and PIV System Challenges

Issues & Challenges	How Smart Cards Help Address PIV System Issues & Challenges
Inadequate security and privacy	• Smart cards strengthen the PIV system's ability to protect individual privacy and secure personal information, providing authenticated and authorized information access, and providing secure on-card storage of private information. • Smart cards provide strong PIV 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 verification. • 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 PIV. • Smart cards provide strong PIV card security, supporting features that deter counterfeiting and thwart tampering. • A single smart PIV card used for logical access can store passwords, PINs, and/or certificates securely and support single sign-on capabilities.
Difficult credential management	• A single smart PIV card can support multiple applications, simplifying the identity verification process for security staff, PIV system administrators, and individuals. • The use of smart PIV 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 PIV 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 PIV card can support multiple applications, replacing multiple, hard-to-manage PIV cards and implementing more straightforward logical access applications.
Proprietary and inflexible PIV 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 PIV 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 PIV cards, reducing overall cost and providing improved efficiencies in PIV verification processes.
Usability problems	• Smart cards supporting multiple applications on single PIV 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.

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

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

"Secure Identification Systems: Building a Chain of Trust"; Smart Card Alliance; March, 2004.

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

Acknowledgements

This document is based almost entirely on a report entitled, “Secure Identification Systems: Building a Chain of Trust” and published by the Smart Card Alliance. The purpose of that report is to discuss the issues with current identity verification systems and to define the role that smart cards play in improving the accuracy, security and privacy of secure PIV systems. It is available in its entirety from the Smart Card Alliance, 191 Clarksville Rd., Princeton Junction, NJ 08550. Contact www.smartcardalliance.org to purchase the full report.

NIST wishes to thank Randy Vanderhoof, Executive Director of the Smart Card Alliance, for granting permission to use their copyrighted report as the primary foundation of this document. We also thank Cathy Medich, Chair of the Task Force that created the report, for providing an electronic copy for adoption and revision.

The SCA report was created by participants from 23 organizations 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

.

Appendix A: Federal Projects using PIV Smart Cards

Several government organizations are working on improving the security and accuracy of their personal identity verification systems. This appendix includes brief summaries of projects implementing new secure PIV systems or who are developing improved PIV trust models.

- 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

U.S. Department of Defense Common Access Card[1]

One PIV smart card program is the U.S. Department of Defense (DoD) Common Access Card (CAC). This PIV card will serve as the DoD standard identity verification and physical access credential in automated turnstiles for controlled access to DoD facilities. The card is currently used for secure PIV 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. 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.

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.

As the CAC identity credential is now being issued to all active military, DoD is beginning to concentrate on incorporating the CAC into many other DoD applications.

Federated Identity and Cross-credentialing System (FiXs)/Defense Cross-credentialing Identification System (DCIS) Proof of Concept[2]

The Department of Defense has 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 by DoD and its contractors that need employee identity verification.

The FiXs/DCIS project will enable participating DoD facilities to achieve strong PIV of participating contractor personnel who present a company-issued trusted credential token. Similarly, participating locations will also recognize a DoD-issued Common Access Card.

A primary goal of FiXs/DCIS is interoperability among many DoD components and PIV token issuers. Interoperability is achieved via a

[1] 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.

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

common trust exchange policy, operating rules and technical specifications that allow various parties to act and exchange information. 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 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 "proven" using several forms of source identity documents, and biometrics are captured. When participants present themselves at a FiXs/DCIS-enabled facility, their identity can be verified.

Transportation Security Administration Transportation Workers Identification Credential (TWIC)[3]

The Transportation Security Administration (TSA) is mandated by federal legislation to develop a PIV 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 PIV of transportation workers and access control for transportation facilities. Current estimates are that 12 to 15 million workers will require the 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.

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

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 are planning a seven-month prototype phase which will begin in early 2004 and will introduce biometric identifiers and contactless technology.

United States Passport: Concept of Operations for the Contactless Chip[4]

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 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

The International Civil Aviation Organization (ICAO) has developed a set of specifications that involve the inclusion of an electronic chip in passports which would store both the facial image and biographic data of the bearer. This is the same data currently found on the data page of a passport.

An electronic passport 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. This 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.

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.

[4] 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.