The Commercial Identity Verification (CIV) Credential – Leveraging FIPS 201 and the PIV Specifications: Is the CIV Credential Right for You?

A Smart Card Alliance Physical Access Council White Paper

Publication Date: October 2011
Publication Number: PAC-11003

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

TABLE OF CONTENTS

1 Introduction

Homeland Security Presidential Directive 12 (HSPD-12) mandates a standard for a secure and reliable form of identification to be used by all Federal employees and contractors. Signed by President George W. Bush in August 2004, HSPD-12 initiated the development of a set of technical standards and issuance policies (referred to as FIPS 201)[1] that create the Federal infrastructure required to deploy and support an identity credential that can be used and trusted across all Federal agencies, regardless of which agency issues the credential.

This credential, the Personal Identity Verification (PIV) card, is now deployed and used by Federal agencies to assign controlled resource access privileges to Federal employees and to authorize the cardholder to access both physical and logical resources. The success of this program is largely due to the development of goals, issuance policies, and technical specifications that all agencies agree to follow. A cross-certification policy establishes trust between agencies, so that employees from one agency can use their PIV credentials to access controlled resources while visiting other agencies. Products and systems that conform to the defined technical interoperability standards are offered by a variety of suppliers. New standards-compliant products are introduced frequently. Today, well over 5 million PIV cards have been issued by the Federal government to employees and contractors.

As the benefits of a common identity credential become clear, interest is growing among non-Federal issuers. PIV-interoperable (PIV-I) cards are already being issued by Federal contractors to those employees who need access to Federal buildings and networks. The PIV-I credentials are technically interoperable with the PIV infrastructure. PIV-I issuers comply with the identity-proofing, registration, and issuance policies described in FIPS 201 and are cross-certified with the Federal Public Key Infrastructure (PKI) Bridge[2] to allow contractor employees to access authorized resources.

Private enterprises can also take advantage of this technology. This white paper defines the Commercial Identity Verification (CIV) credential, which leverages the PIV-I specifications, technology and data model without the requirement for cross-certification. Any enterprise can create, issue, and use CIV credentials according to requirements established within that enterprise's unique corporate environment.

This white paper was developed by the Smart Card Alliance Physical Access Council to provide guidance on how enterprises can take advantage of FIPS 201 and the PIV credential specifications to implement a standards-based identity credentialing program. The paper discusses benefits, describes best practices and technical requirements, and provides a set of reference documents to assist corporations in establishing a secure, reliable, electronically verifiable identity program.

[1] U.S. Department of Commerce and National Institute of Standards, *Federal Information Processing Standards Publication: Personal Identity Verification (PIV) of Federal Employees and Contractors,* FIPS Pub 201-1, March 2011.

[2] http://www.idmanagement.gov/pages.cfm/page/Federal-PKI

2 Overview: The CIV Credential

Over the past 10 years, the Federal Government has developed, tested, and refined both PIV and PIV-I credentials. The PIV credential is issued to virtually all qualified government employees, who use it for physical access to government buildings and facilities, to log on to their computers, and to access controlled Web sites.

Both credentials are currently available as smart cards. The computer chip embedded in the card enables the credential to perform cryptographic processes that provide strong resistance to tampering, duplication, and counterfeiting and enables strong authentication processes when using the credential to access protected facilities and networks. The result is enhanced protection of personal privacy, reduced identity fraud and enhanced security.

One of the main advantages of these credentials is that they adhere to a set of standards that is accepted by suppliers, issuers, and users. Previously, most access control systems relied on vendor-specific proprietary identity credentials. Interoperability was typically confined to a few office sites belonging to a single organization. A standards-based credential means that any government employee's credential can be accepted by any government facility and IT network. In addition, vendors of both logical and physical access control products can build equipment that complies with one common standard. As a result, the Federal government can now choose from a wide range of conforming access control products, which can be purchased from a variety of suppliers, and be assured that their choice will work with every employee's or contractor's credential.

The same opportunities are now available to the commercial market. This white paper defines a new credential that leverages the PIV specifications—the CIV credential. Enterprises that use this credential and access control products built to support the PIV-I credential can achieve levels of access control security and technical interoperability similar to those available using PIV cards.

The CIV credential is technically compatible with the PIV-I credential specifications. However, a CIV credential issuer need not comply with the strict policy framework associated with issuance and use of the PIV and PIV-I credentials. This freedom allows corporate enterprises to deploy the standardized technologies in a manner that is suitable for their own corporate environments.

2.1 Corporate Benefits of Adopting the CIV Credential

Currently, companies often create multiple identities for each individual. Each identity is established by a different campus or office location within the company. The locally-issued identity credential is designed to be compatible with local access control systems and grants access to various local resources, both physical and logical.

Deciding to adopt the use of a CIV credential can be the first step a company takes in aligning the hiring process with identity and access management best practices. Establishing a central identity management solution means that each individual cardholder has one corporate identity and one identity credential, which allows specific access across corporate-wide logical and physical resources (Figure 1). Each employee can be issued a single identity credential to be used corporation wide, rather than having to obtain different credentials that often must be established to access multiple logical resources and used at every different corporate location.

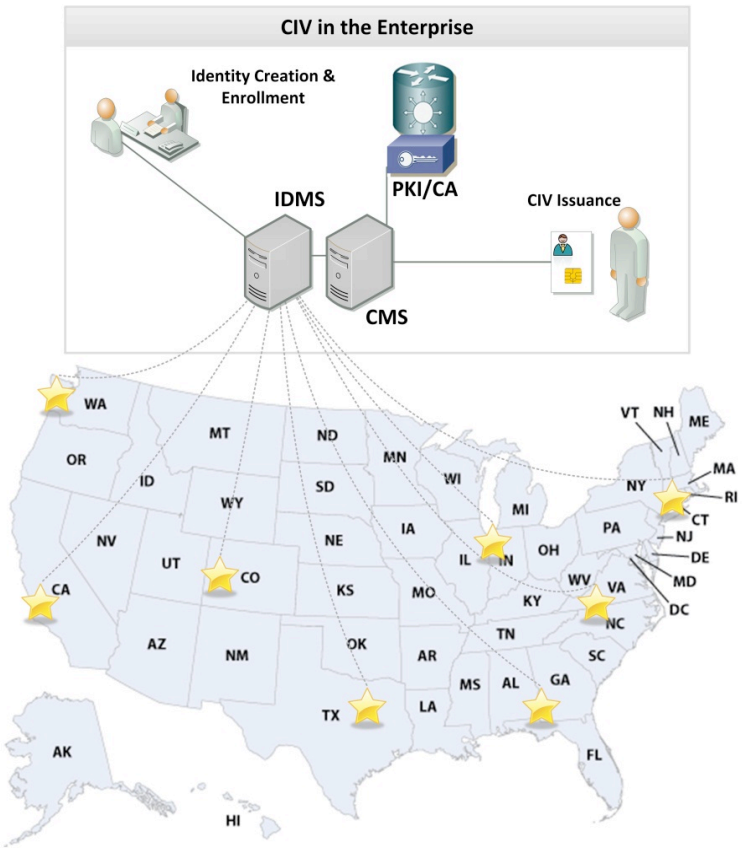

Figure 1. Enterprise CIV Credentialing Implementation with Multiple Locations

A commercial enterprise that uses a CIV card as the combination identity and access card for both logical and physical access can capitalize on the lessons learned from the Federal government. In addition, such companies will be well positioned to streamline their business processes for convergence of physical and logical security, reducing redundant access management activities. Using a standards-based solution for both physical and logical access eliminates the need to manage separate access verification processes and allows for automated revocation of access privileges when an employee leaves the company or the credential expires.

Modern operating systems such as Windows 7® include enhanced support for smart card-related plug-and-play operation and the PIV standard.[3] This means that a technically conformant identity credential such as the CIV credential can be authenticated and validated as an integral part of the normal log-on procedure. The benefit is a reduction in unauthorized network access and no requirement to manage and frequently change log-on passwords.

The CIV credential provides the foundation for interoperable solutions using commercial off-the-shelf (COTS) products that are offered by multiple vendors. Competition for sales will continue to reduce product cost.

[3] http://technet.microsoft.com/en-us/library/dd367851(WS.10).aspx

2.1.1 Corporate Use Case

The following example illustrates the use of a central identity management system that issues a CIV card establishing one identity per employee or contractor.

Each CIV card contains one unique user identification number. When an employee or contractor receives a CIV card, the card is provisioned with the cardholder's credential number, which is tied to that person's network account and authorized applications and to the physical access control systems (PACS) in the appropriate buildings. The cardholder then uses the new card to access the door of the building or the office suite, or to logon to computers and networks.

The single CIV credential can work at campuses across the enterprise. Personnel can move from one company location to another, using their CIV cards to confirm their corporate identity and have privileges assigned quickly. This flexibility is especially beneficial for companies with multiple facilities spread nationwide or even globally.

The enterprise may use the CIV credential as a tool to establish a single sign-on policy. Once the cardholder is logged onto an authorized corporate computer, the person can access all required applications without additional authentication requirements. Single sign-on simplifies password management and reduces the requirement on both the help desk and users to manage multiple passwords. The CIV credential can also be configured to enable remote logical access for employees working from home who access their logical resources through a company virtual private network (VPN).

Each employee's CIV card can be a tool for authenticating identity and authorizing access to resources such as inventory control, accounting, and process control systems and to HR databases. In addition, a single identity allows a provisioning system to confirm that an employee is actually on the premises before enabling that person to log on to a desktop computer and enterprise network, while at the same time blocking access from an external device, such as a remote computer, after physical presence is established within an office.

2.1.2 Physical and Logical Access Use Case

The convergence of physical and logical access control with a centralized identity management system (IDMS)/card management system (CMS) gives an organization the ability to audit and monitor all of their resources in one place (Figure 2). Electronic authentication for access to physical locations can enable organizations to reassign their security resources to activities such as monitoring and auditing, as opposed to conducting visual badge inspections or cross-referencing various databases for a specific event or transaction.

A centralized IDMS/CMS can log both the entrance of a cardholder into a specific location and the person's subsequent network access. If the same CIV credential is used to simultaneously access a corporate office in California and an application in New York, a message can be generated that immediately alerts security. Traditionally, the physical access information and the logical access information would be stored in different databases and monitored by different groups, making it much more difficult to detect suspicious activity.

In addition to monitoring, an organization can audit and report on transactions reliably using one central application. Many COTS products for deployment support auditing and reporting based on a particular credential, location, application, or period of time. The centralized model for CIV credential deployment and maintenance also gives organizations the ability to monitor, audit, and report on a local level. Some enterprises have subsidiary organizations or locations that operate independently; a centralized CIV credentialing system would be configured to include interfaces to established systems and databases such as a human resources, physical security, or domain server.

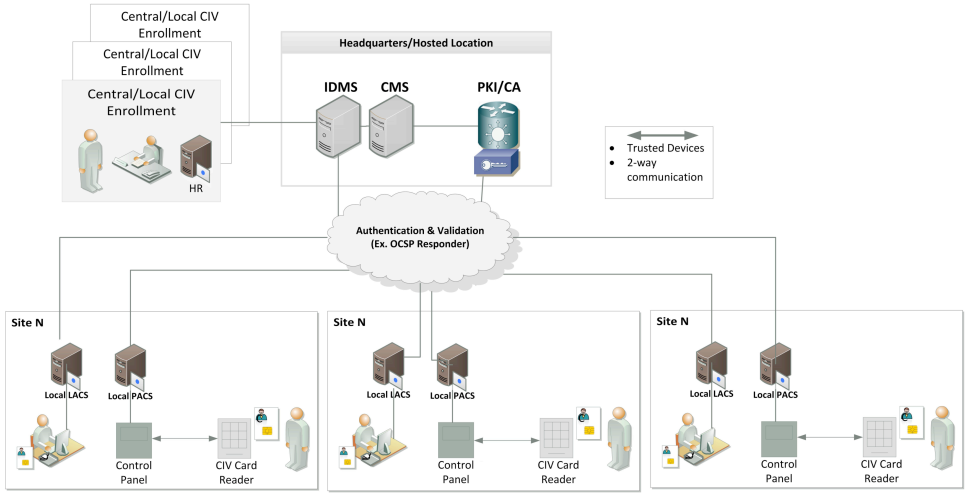

Figure 2. Multi-site Enterprise Network with CIV Credentialing Infrastructure Supporting Local Access Control

2.2 Planning Considerations

The CIV credential leverages the PIV-I standard, which is supported by multiple vendors and is capable of a wide range of business functionality. CIV credential issuers will enjoy the benefits of choosing from standardized products and processes that have been tested, deployed in large quantities, and proven to work. Appropriate enterprise implementation of the CIV credential can be a powerful part of an enterprise identity-security strategy.

2.2.1 Corporate Goals and Objectives

Corporate-wide programs involve multiple stakeholders and interest groups. For successful implementation of a corporate identity credentialing project, all stakeholders should be involved in the process. Involvement includes defining the objectives of the identification program, identifying expected business applications, defining policies and public key infrastructure (PKI) requirements, selecting technology and technology partners, and designing credential management procedures.

All stakeholders must share a clear understanding of the desired outcome. A set of clearly defined goals and objectives is one way to achieve such an understanding across an enterprise.

Examples of strategic objectives for a CIV credentialing program include the following:

- Develop clearly defined processes and capabilities for enabling trust across the enterprise.
- Consolidate credentialing and authentication capabilities.
- Control logical and physical access enterprise-wide.

Examples of goals for a CIV credentialing program include the following:

- Realize cost savings by eliminating enterprise legacy credential systems through use of standards-based authentication processes.

- Exploit economies of scale by leveraging Federal standards for both credentialing and credential validation functions.
- Provide the capability to use credentials across the enterprise.
- Improve privacy and protection of employee personally identifiable information (PII)

2.2.2 Use of Biometric Technologies

Biometric technologies have a valuable place in a secure identity credentialing program. Biometric methods can be used to positively bind an individual's identity to that individual's credential. As an added benefit, biometric binding can prevent use of a lost or stolen card to access corporate resources.

The CIV credential follows the PIV-I specifications for biometric support. Currently, the interoperable biometric that would be stored on the CIV credential for matching purposes is a fingerprint. While a standardized digital facial photo is also stored on the credential, this data record is intended for visual comparison, and although it could be used for automated biometric comparison, it typically is not.

Fingerprint data is stored on the CIV credential in a secure area and conforms to a standardized template format that is processed from the original bitmap image captured during the biometric enrollment process. For privacy reasons, the fingerprint templates stored on the CIV credential can only be accessed through a contact interface after entry of a valid personal identification number (PIN).

2.2.3 Cryptographic Authentication

Strong card authentication using cryptographic functions guarantees that a CIV card is authentic and neither cloned nor altered.

A PIV card carries multiple PKI certificates for various uses. A CIV card needs at least one certificate to support access control with automated deprovisioning; additional certificates are optional. How many to deploy will depend upon the various security use cases the enterprise wishes to support.

Like the PIV card, the CIV card can support multiple levels of authentication to ensure that the credential is genuine and has not been cloned or altered, and to prevent fraudulent use of a lost or stolen credential. For each access control point, either physical or logical, an enterprise chooses an appropriate level of assurance and then chooses a product that can implement this choice.

Cryptographic keys on the CIV credential should be chosen to support various security-related uses cases. Asymmetric cryptographic key options include a signing key (for signing e-mail messages and other documents), an encryption key (to provide privacy for e-mail messages and other documents), a card authentication key (for use with physical or logical access control products over the contactless interface of the CIV card), and a personal identity verification key (for use in access control situations where the cardholder's private information, such as a fingerprint or PIN, must be protected). A symmetric key for use in certain encryption use cases is also an option. At least one asymmetric public key pair will be required for most deployments. (For more information on asymmetric and symmetric keys, see Section 7.)

Several vendors provide systems that can be used to issue and manage CIV credentials (see Section 3.5). The enterprise should consult with these vendors to determine which of the above options are suitable for their use cases

2.2.4 Government Compliance

Using systems and components that were developed to comply with government standards and guidance does not mean than an enterprise must follow government regulations and policies.

The CIV card is technically the same as a PIV-I card but is created without requiring the use of Federal identity vetting policies or adherence to the staffing, workflow, issuance, and activation policies required to issue a PIV-I credential. However, these policies and procedures are required of PIV-I issuers to achieve cross certification to the Federal PKI Bridge and to enable credentials to be trusted across organizations.

CIV issuers can define their own procedures, tailored to their own corporate business roles and workflow, for creating a CIV credential that can be authenticated and trusted across their enterprise and be read by equipment that can read and process PIV-I cards.

The CIV credential does not need to comply with all of the PIV policy standards. The identity verification process can be the process defined for PIV-I, or a company can continue to verify the identity of employees using its current procedures. The CIV model does not require a trusted PKI infrastructure outside the company itself, simplifying certificate authority management and certification.

Because the CIV processes rely on the same techniques and technical components as the PIV credential, it will be easy to migrate from use of a CIV credential to use of a PIV-I credential. This ease of migration can be valuable for enterprises with personnel who are required to interact on a regular basis with the Federal government.

2.3 Summary

A CIV credentialing program offers a corporate enterprise numerous advantages. To determine whether CIV is an appropriate choice, a corporate enterprise needs to ask the following questions:

1. Is the current level of security at the corporation satisfactory?
2. Are only those authorized to do so accessing the corporate campus and networks?
3. Are there vulnerabilities in corporate computer networks, access control systems, or other corporate systems that expose the corporation to security risks?
4. Are inappropriate amounts of money and resources devoted to supporting the corporate networks?
5. Are employees' privacy rights protected?

A corporate enterprise that chooses to implement a CIV credential will realize the same cost savings as Federal agencies and contractors. A CIV credentialing program provides a corporate enterprise with the ability to improve efficiency and reduce resources while sustaining and maintaining security at both physical and logical access points. The return on investment is realized quickly: physical access points require fewer personnel, and there is a significant decrease in the requirement for user assistance for logical access (for example, to provide forgotten passwords and unlock locked accounts). Operations become more streamlined and security more robust.

One size does not have to fit all. A corporate enterprise can use the supporting technology and standards in the way that best fits the enterprise's requirements. The CIV issuance process and lifecycle support can be tailored to each corporation's business roles and workflow, while the CIV cardholder takes advantage of the same rapid electronic authentication capabilities as PIV and PIV-I cardholders and is protected by the highest levels of security.

In short, the CIV credential provides a corporate enterprise with enhanced security, improved data protection, more secure networks and physical facilities, increased cost savings, and improved efficiency.

3 Implementation Considerations and Best Practices

CIV credential deployment involves five primary steps:

1. Define the business applications to be supported in the enterprise.
2. Define the identity policies to be enforced.
3. Deploy a PKI for issuing digital certificates.
4. Deploy a CMS for managing smart cards and certificates.
5. Deploy the CIV cards.

Multiple component vendors and Internet-based cloud solutions can assist with the last three steps. Thanks to the PIV and PIV-I standards that the CIV credential is based upon, the components in these three steps are relatively standardized. Any business application can be supported and any identity policy can be enforced by any compliant technology. Any PKI can be used with any CMS and any CIV card. This interchangeability is the greatest strength of the CIV model, and is enabled due to the CIV infrastructure being based on open standards.

The remainder of this section highlights different steps involved in implementation, discussing deployment considerations and challenges. Numerous experts (both individuals and organizations) can help evaluate possible options and select the best choices.

3.1 Define the Business Applications to be Delivered

Any CIV implementation must start with business applications. One of the strengths of PKI and smart card technologies is that they provide security that is almost impossible to bypass. However, there is a drawback associated with that strength, in that applications that are not supported in the original system design may be impossible to support without upgrades, reconfiguration, or card replacement. It is critically important to ensure that all anticipated applications are considered, engineered, and tested prior to rollout, but particularly applications in the following categories:

- PACS applications
- Applications using biometrics
- Logical access control/computer strong authentication applications
- Digital signatures
- Applications using digital encryption

Applications to be delivered must be engineered and tested to ensure that they will work after deployment. Most problems with smart card deployments stem from shortcomings in this planning process. Adding a new class of business application after deployment may require replacing parts of the infrastructure, replacing the already-deployed smart cards, or both, frequently resulting in considerable delay, cost, and frustration. Proper planning for the types of business applications to be supported can prevent these issues.

3.2 Define Security Policies

Security policies have two purposes:

- To define the types of credentials to be issued and the levels of assurance that the credentials represent

- To enforce policies and procedures for credential issuance and modification that ensure the integrity of all credentials over their life cycle

What security policies are chosen for the CIV credential are entirely up to the issuing organization. However, it is important to consider policy factors early, to ensure that the implementation adequately enforces the chosen policies. A system that is built to enforce one security policy may be difficult to modify to support a different or changed policy, so initial caution and careful thought are recommended. Two other considerations are worthy of mention:

- The Federal PIV and PIV-I communities have created some excellent examples of security policies, and these policies can serve as a starting point for organizations to tailor to fit the corporate environment.
- If interoperability with other organizations is an objective, the security policies of both organizations must be considered and coordinated to enable credential recognition across organizations.

3.3 Deploy PKI

PKI is widely regarded as "the technology that secures the Internet," and it is critical to a CIV credential deployment.

3.3.1 Approaches to PKI

Four main approaches can be considered when deploying the PKI:

- Use an external, shared service provider.
- Use an externally hosted, private service provider.
- Use a locally hosted, private infrastructure.
- Participate in PKI bridges for external interoperability.

Each approach involves particular considerations.

The first two approaches rely on the expertise of an external provider, such as VeriSign, Verizon Business, Entrust, or others, to ensure proper configuration and security of the PKI and its operation. In this shared environment, multiple customers rely on a single infrastructure, which can limit flexibility.

When a private service provider is used, resources are dedicated to a single organization, resulting in greater flexibility but at a correspondingly greater cost. With a private infrastructure, the PKI is fully customizable but requires a dedicated infrastructure and staff to maintain it.

Participation in external bridges can enable trust across organizations and federated identities, but at the expense of greater complexity, cost, and the limited flexibility that can be imposed by the necessity to agree on and share policies.

3.3.2 Certificate Authorities

The critical component of an enterprise PKI is the certificate authority (CA). A corporate CA is responsible for the entire life cycle of the certificates it issues. The CA publishes details about its internal procedures in a certificate policy (CP). Relying parties (the users of the certificates) can then decide for themselves how trustworthy the CA and its certificates are. The degree of trust is often referred to as a "level of assurance."

A CA can offer more than one level of assurance, depending upon the intended uses of its certificates. Certificates issued to other CAs (CA certificates), for example, require a much higher

level of assurance than certificates issued to individuals. Each level of assurance is associated with a set of minimum procedural requirements that is described in the CP and is assigned a policy object identifier (OID). When the CA issues a certificate, it includes one or more policy OIDs, which describe the purposes for which that certificate can be used.

A CA cannot control how a relying party uses one of its certificates. It can only attest, through the use of policy OIDs, the circumstances around which the certificate was issued. The relying party is ultimately responsible for deciding how to treat OIDs, based upon its interpretation of the CP.

3.4 Deploy CMS

The CMS is a critical component of CIV credential deployment, because it acts as the bridge between the PKI that generates user credential certificates and the cards that store those certificates and their private keys. The CMS allows administrators to identify users, program electronic identities onto cards, administer and update cards after they have been issued, and retire/revoke cards that are lost or no longer needed.

In addition, the CMS serves as the "brain" of the smart card program for the purposes of integration with other systems, policy enforcement, and auditing and investigation. Finally, depending on how the smart cards are to be used, the CMS can serve as the integration point with numerous optional components, including badge printers, biometric readers, PACS, and logical access applications (e.g., one-time-password tokens).

As is the case for PKI, the CMS can be provided as an external hosted service, although external card management system providers are not as well-established as external PKI service providers. When selecting a CMS or a CMS service, it is important to consider the corporation's business needs and the integration points required to fulfill those needs. Corporations should therefore consider the following factors:

- Compatibility with the corporation's identity management systems
- Required integration with PKI service providers
- Required integration with badge/card printing and production processes
- Support for additional features, applications and options, such as biometrics or one-time-password tokens
- Ability to enforce the desired enterprise policies

3.5 Deploy CIV Cards

When the previous steps have been undertaken carefully, deploying the cards themselves should be the easiest step of all. Thanks to the smart card industry's support of the FIPS 201 standards and PIV specifications, there can be considerable standardization among CIV cards from the different vendors, assuring a baseline level of compatibility and interoperability among all of them. GSA maintains a list of approved vendors; although private organizations cannot purchase through GSA, they can access the GSA approved products and services list[4] to locate qualified vendors.

At the same time, there are differences among vendors, card models, and card features, and thought must be given to balance desired features, technology choices, and costs. Key considerations include the following:

- Inclusion of PACS technologies

[4] The list is available at http://fips201ep.cio.gov/apl.php.

- Inclusion of legacy technologies such as magnetic stripes
- Visible and invisible security features, including holograms and overlays
- Use of contactless and dual-interface smart card technologies
- The capacity and features of the smart card chip itself
- Pre-personalization of chip data and manufactured card printing
- Options for personalization and shipping of completed cards
- Cost

Key considerations are card personalization and issuance. Some companies may want to manage their own local CIV card personalization and issuance, while others may choose to outsource these processes to a personalization and issuance vendor. The decision will depend on the organization's security and policy requirements, the size and the maturity of their enterprise, and the cost differences between insourcing and outsourcing.

3.6 Summary

The decision to implement the CIV credential must be a corporate-wide decision that involves all of the stakeholders from the beginning. Planning must include careful analysis of business applications and security policies.

Numerous service providers can perform some of the processes required to issue and support CIV cards. Each provider has a unique approach and level of service. Smart card manufacturers have the ability to perform all aspects of card manufacturing, programming, personalization, printing, shipping, and delivery. Service providers offer both fully hosted and hybrid personalization and issuance solutions in which an enterprise subscribes only to the specific functions it requires.

However, the most careful consideration must be given to the business applications to be delivered and the security policies to be enforced. Balancing these factors with organizational needs and costs will deliver a card with the greatest value.

4 Overview of PIV-I and CIV Credentials

In May 2009, the Federal CIO Council released *Personal Identity Verification Interoperability for Non-Federal Issuers*.[5] This document lays the groundwork for use of the FIPS 201 standard and supporting documentation by organizations that are not part of the Federal Government.

4.1 Comparison of PIV-I and CIV Credentials

Table 1 summarizes the similarities and differences between the PIV, PIV-I, and CIV credentials.

Table 1. Comparison of PIV, PIV-I and CIV Credentials

	PIV	PIV-I	CIV
Policy			
Identity vetting Breeder documents Background checks	Follows FIPS 201	Requires two breeder documents defined by FIPS 201 Other policies are defined by the issuer with the intent to be cross-certified by the Federal Bridge	Follows the corporation's policies
Process			
Enrollment Issuance Activation	Follows FIPS 201	Follows FIPS 201	Follows the corporation's policies
Technical Interoperability			
Card data model	Follows SP 800-73*	Follows SP 800-73*	Follows SP 800-73*
Credential number	FASC-N	UUID	UUID

* FIPS 201 currently allows optional use of certain SP 800-73 data objects. Should an enterprise choose not to use all SP800-73 data objects, technical interoperability between the card and the card reader requires that any data objects that are not used must be identified as not populated.

A central authority ensures that Federal issuers issue credentials with a unique identifier. The presence of this authority mitigates the risk that cards issued by separate, independent Federal issuers will have duplicate credential numbers. However, no central authority exists for non-Federal issuers. To enable private enterprises to generate their own universally unique identifier (UUID) numbers with minimal risk of duplication, PIV-I generates the number using a method described in the *Personal Identity Verification Interoperability for Non-Federal Issuers.*[6]

The policies related to issuance and personalization of PIV-I cards are essentially the same as those for a PIV card, although there are some technical differences. In particular, to prevent identifier collisions with credentials issued by the Federal government, PIV-I and CIV cards

[5] Federal CIO Council, *Personal Identity Verification Interoperability for Non-Federal Issuers*, July 2011, http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf
[6] Ibid.

should not use the Federal Agency Smart Credential Number (FASC-N); instead, the issuer generates an RFC 4122-compliant Global Unique Identifier (GUID) to be used as the credential identifier. In addition, CIV issuers need not follow certain other requirements to cross-certify their CIV credentials with the Federal PKI Bridge for interoperability with the PIV cards and use within Federal agencies.

In addition, as with the PIV-I card, the printed CIV card should visually look different than a PIV card.

4.2 Comparison of CIV and Proprietary Solutions

Using a CIV card instead of another proprietary product or design offers a corporate enterprise several important advantages:

1. Cards, systems (CMS and card personalization systems (CPS)), and readers are commercially available from multiple vendors (see Section 3.5).
2. The best practices derived for the CIV model are designed to prevent fraud, protect privacy, and provide a standards-based solution that should be less expensive to maintain and evolve over time.
3. Technical interoperability of installed readers and infrastructure (for logical access control systems as well as PACS) allows readers to accept credentials from an increasing variety of issuers who are using the PIV and PIV-I standards (such as government agencies, government contractors, and states issuing First Responder Authentication Credentials).

Technical interoperability is a critical advantage. The term refers to the ability of a reader to work with a PIV, PIV-I, or CIV credential without requiring a software change. The CIV credential is issued by the owner of the reader (essentially a closed application), and there is no need to extend trust among independent entities (as in PIV or PIV-I), reducing constraints on issuance processes, identity vetting policies, and PKI requirements.

CIV issuers can chose from a variety of products (CMS, CPS, readers, and applications) without having to define a unique corporate data model or credential. A CA would be incorporated under the direct control of the issuer without any need for external interoperable trust.

It must be noted that the CIV model cannot be identical to the PIV or PIV-I model. Any data object added to the CIV model should have a private ASN.1 tag and not use a tag within the name space used by NIST and ISO (both use the ASN.1 application class). This is to protect any modification by the CIV issuer from ever risking a collision with future versions of PIV or ISO specifications.[7] Equally important, the OIDs used in the CIV certificates must be different than the PIV or PIV-I OIDs and based on or generated by the CIV issuer's own data structures and identifiers.[8]

4.3 Influence of Evolving Standards

One of the more common reasons given for not adopting CIV credentials is that standards keep evolving. This normal evolution of standards raises an issue: how can a corporation be sure of compliance once its CIV infrastructure is in place and the CIV credentials are ready for deployment? In other words, how can a corporate enterprise implement the CIV credential in a way that will guarantee that the credential will not be obsolete once it is deployed?

---

[7] For more information about private ASN.1 tags, see Section 3.1 of the document at http://luca.ntop.org/Teaching/Appunti/asn1.html

[8] For more information about OIDs, see http://standards.ieee.org/develop/regauth/tut/oid.pdf

Companies adopt technology to meet specific business needs. For example, computers become obsolete very quickly, but even "obsolete" computers can satisfy an organization's business requirements for a number of years. If organizations waited to buy computers until computers stopped evolving, no organization would ever buy a computer.

The same principle applies to smart card-based identity credentials. To address the issue of potential obsolescence, corporations should incorporate into their implementations only those portions of the PIV standards that are required to meet their business requirements. Unlike the government, private enterprises are not required to achieve PIV compliance with their CIV credentialing programs. A CIV corporate credentialing program can use the FIPS 201 technical standards as a foundation, while creating the issuance and usage policies appropriate to their own environment.

In selecting which PIV standards to adopt, corporations should consider the two main reasons for using standards-compliant equipment:

1. Such equipment can be sourced from multiple suppliers, mixing and matching components with the knowledge that components will work together.
2. Standards support backward compatibility. When NIST changes a standard, the new standard always supports the core functions developed in previous versions. The standards updates simply add new functionality (for example, in the draft FIPS 201-2, allocating space for old PKI certificates and private keys to decrypt data that was encrypted with old keys).

4.4 Form Factors

FIPS 201, Special Publication 800-73 and Federal CIO Council PIV-I guidance require PIV and PIV-I credentials to comply with ISO/IEC Standard 14443 Parts 1-4, a contactless smart card standard. The CIV credential will follow ISO/IEC 14443 as well. ISO/IEC 14443 Part 1 references ISO/IEC 7810, which defines the form factor as a credit card-sized plastic card. Therefore, PIV, PIV-I and CIV credentials, as specified by the standards, are restricted to the card form factor.

Credentials based on smart card technology can be available in a variety of form factors. While most smart identity credentials are commonly delivered as a plastic card, smart credential technology is also available in smart phones, key fobs, USB tokens, and wristwatches. The benefits and value propositions for each form factor vary, depending on the credential holder's role (e.g., citizen, government employee, enterprise employee, student).

ISO/IEC 14443 is currently under review by the INCITS B10.5 committee[9] to determine how new use-case requirements, including alternate form factors, can be accommodated.

[9] http://standards.incits.org/a/public/group/b10.5

5 Conclusions

A corporate enterprise can choose to implement a CIV credentialing program in many different ways, some more costly than others. Regardless, however, the baseline is the same: to decide on a CIV identity credentialing system requires defining objectives, identifying expected business applications, examining PKI infrastructure and associated policy requirements, and deciding on technologies, technology partners, and credential management procedures.

Before initiating a CIV implementation, corporations must decide as a critical first step which applications are required. Applications can include physical access control; biometrics; logical access control/computer strong authentication; digital signature; and digital encryption. Once the applications are identified, security and other policies can be defined.

While technology and standards keep changing and evolving, the business applications that make deploying a CIV credential desirable do not. If a corporate entity implements CIV credentials to meet its business requirements, maturing standards and technologies will only enhance the quality of the system.

6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Physical Access Council to provide guidance on how enterprises can take advantage of FIPS 201 and the PIV credential specifications to implement a standards-based commercial identity credentialing program. The white paper defines the Commercial Identity Verification credential as a credential that uses the same technology and data model as the PIV-I credential.

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

The Smart Card Alliance thanks the Council members for their contributions. Participants involved in the development of this white paper included: ActivIdentity; AMAG Technology; Bioscrypt/L-1 Identity Solutions; Booz Allen Hamilton; Codebench, Inc.; Datacard Group; Datawatch Systems Inc.; Diebold; E & M Technologies; HID Global; Hirsch Electronics; HP Enterprise Services; IDenticard; Identification Technology Partners; IDmachines; Intellisoft; NagraID Security; NXP Semiconductors; Roehr Consulting; SAIC; SCM Microsystems; Tyco Software House; Unisys; U.S. Department of State; XTec, Inc.

Special thanks go to **Lars Suneborn**, Hirsch Electronics, who managed the project and to **Gilles Lisimaque**, Identification Technology Partners, **Lolie Kull**, HP Enterprise Services, and **Chris Williams**, SAIC, who made major contributions to the development of the white paper.

The Smart Card Alliance thanks the following Council members who wrote content for this document:

- **Mari Devitte**, XTec, Inc.
- **Bob Dulude**, ActivIdentity
- **Bob Fontana**, Codebench
- **Walter Hamilton**, ID Technology Partners
- **Kevin Kozlowski**, XTec, Inc.
- **Lolie Kull**, HP Enterprise Services
- **Gilles Lisimaque**, ID Technology Partners
- **Roger Roehr**, Roehr Consulting
- **Steve Rogers,** Intellisoft
- **Jean Schultz**, E & M Technologies
- **Adam Shane**, AMAG Technology
- **Lars Suneborn**, Hirsch Electronics
- **Chris Williams**, SAIC

The Smart Card Alliance also thanks the Council members who contributed during the document review, including:

- **Sal D'Agostino**, IDmachines
- **Tony Damalas**, Diebold
- **Frazier Evans**, Booz Allen Hamilton
- **Tony Ferguson**, Bioscrypt/L-1 Identity Solutions
- **Marty Frary**, Independent
- **Dan Hudson**, Datacard Group
- **Brent Iles**, Datacard Group
- **Jeff Johnson**, Unisys
- **Russ Kent**, HP Enterprise Services
- **Diana Loughner**, IDenticard
- **Stafford Mahfouz**, Tyco Software House
- **Don Malloy**, NagraID Security
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, SCM Microsystems
- **David Nichols**, HID Global
- **Zeca Pires**, Datacard Group
- **Rick Pratt**, XTec, Inc.
- **Kenny Reed**, Datawatch Systems Inc.
- **Dan Schleifer**, IDmachines
- **Mike Sulak**, U.S. Dept. of State
- **Rick Uhrig**, XTec, Inc.
- **Mike Zercher**, NXP Semiconductors
- **Rob Zivney**, Hirsch Electronics
- **Ryan Zlockie**, Datacard Group

About the Physical Access Council

The Smart Card Alliance Physical Access Council is focused on accelerating widespread acceptance, use, and application of smart card technology for physical access control. The Council brings together leading users and technologists from both the public and private sectors in an open forum and works on activities that are important to the physical access industry and addresses key issues that end user organizations have in deploying new physical access system technology. The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software, and reader vendors; physical access control system vendors; and integration service providers.

7 Appendix A: Considerations and Best Practices for Card Authentication Key Implementation

Commercial organizations deploying CIV credentials to protect physical and logical resources can use the Card Authentication Key (CAK) to perform strong authentication. (Authentication is the process that establishes confidence in user identities.) Organizations can leverage the CAK to protect themselves from fraud, tampering, and counterfeit cards. Strong authentication of a CIV credential should include cryptographic functions.

Two major types of cryptographic functions are possible to support CAK authentication: symmetric and asymmetric. Asymmetric cryptography uses two related keys, a public key and a private key, to perform complementary operations. Symmetric cryptography uses a shared secret cryptographic key to perform the cryptographic operations. Any symmetric key implementation should follow best practices and diversify the keys in the cards. Both symmetric and asymmetric methods allow for strong authentication; both methods meet the highest level of assurance defined by SP 800-63, *Electronic Authentication Guideline*.[10] While both offer the same level of assurance, the required steps and use for each differ.

While asymmetric cryptography is necessary to authenticate the use of X.509 digital certificates, CIV credentials can support both a symmetric and an asymmetric CAK, and there are instances where organizations should use symmetric authentication to increase efficiency without compromising assurance and security.

Symmetric cryptography is ideal when most of the cardholders entering a building are individuals who are connected with the commercial enterprise and are presenting an organization-specific CIV credential. In these cases, employing symmetric cryptography can decrease the time it takes to complete a transaction while still ensuring that the individual presenting the CIV credential is who that individual claims to be and that the CIV credential is genuine. Symmetric card authentication also provides commercial organizations with a strong level of autonomy for physical access control. This may be necessary in instances where the organization wishes to allow employees only into specific buildings or building areas.

Asymmetric cryptography is widely accepted as an open and sound means of authentication. Any commercial organization considering technical interoperability should include an asymmetric CAK. In order to perform strong authentication, access control systems must complete four major authentication steps.

1. Verify that the unique ID on card is not altered and that it is signed and trusted.

   Action: Check the cardholder unique ID (CHUID) to ensure that it is signed and matches the unique ID on the digital certificates.

2. Ensure that the certificate belongs to that specific card.

   Action: Perform a challenge-response exchange. The challenge is a random number sent to the card, to which the card responds by encrypting the random number using its unique private key, allowing the result to be verified using the same card's public key.

3. With the legitimacy of the certificate and card confirmed, now ensure that the certificate is active and has not been revoked.

   Action: Check the status of the digital certificate using the Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) responder.

[10] NIST, SP 800-63, *DRAFT Electronic Authentication Guideline, Rev. 1*, June 28, 2011, http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1-Draft3_June2011.pdf

4. Ensure that the entire certificate chain is trusted and legitimate and that no root or intermediate key certificate has been revoked.

   Action: Perform path validation. Review the chain of issuers to determine that all are legitimate and trusted.

Failure to complete all four steps when conducting asymmetric cryptography results in vulnerabilities that can be exploited, such as counterfeit credentials or credentials that have been revoked by the issuing entity. Because asymmetric cryptography keys are longer and the process involves more steps, transactions require more time to complete; if an organization deploys asymmetric cryptography, it should be prepared to conduct asymmetric cryptography for physical and logical access as practically and efficiently as possible. Some methods for practical and efficient asymmetric cryptography include the use of edge devices, such as a validation responder placed close to access points, and the use of cloud technology.

The CAK provides a strong authentication factor, but it is based on the "what you have" factor and does not authenticate the legitimacy of the cardholder. Therefore, the card can be used by anybody. If user authentication is required, verification of the "what you know" factor (e.g., a PIN) or "who you are" factor (e.g., biometrics) or both would also be necessary.

8 Appendix B: Biometrics and Smart Card Technology – Additional Implementations

When used in conjunction with a smart card, biometric technology can provide a very high level of assurance for confirming an enrolled individual's identity. While a fingerprint is the default biometric data defined in FIPS 201, an enterprise can use other biometrics that are not specified by FIPS 201, such as iris patterns, facial images, hand geometry, and vein patterns.

For privacy reasons, organizations may want to consider how biometric data is stored and accessed. Based on the PIV data model, access to the fingerprint templates stored on the CIV credential is only allowed through the contact interface and requires prior entry of a PIN. If there is a requirement for matching biometrics using the contactless interface without PIN entry (as in some PACS), then the biometric can be enrolled separately and stored off the card (e.g., in a card reader or access control system). In this case, the UUID on the CIV card acts as a "pointer" to the biometric record stored in the external system. Using this approach, any biometric modality can be used (fingerprint, iris, face, vein) and stored in the PACS, but the biometric may or may not conform to interoperability standards.

Future NIST PIV specifications may include a secure communication channel between the PIV credential and the reader, to enable biometric matching using the contactless interface with no requirement for PIN entry while still protecting the privacy of the biometric data exchange.

It is expected that future versions of the FIPS 201 standard will permit the optional storage of standardized iris templates as well as on-card matching of standardized fingerprint templates. CIV credential implementers could then choose to follow the changes in the standard.

Biometrics can be used in a wide variety of applications (Table 2) as a second or third authentication factor, providing stronger assurance that an individual's identity is accurately verified.

Table 2. Potential Uses and Benefits of Biometric Data

Application	Benefit
User identification User verification Physical access Logical access	Always with you Convenient Easy to use

9 Appendix C: Data Models

The CIV data model is based on the PIV data model specified by NIST SP 800-73-3.[11] This publication provides PIV card technical interoperability specifications. CIV cards and PIV-I cards adhere to the NIST SP 800-73 data model.

One advantage of following the current PIV data model is reusability and interoperability. Processes, workflows, and techniques are quickly integrated into a CIV credentialing system with a fraction of the engineering work that was needed to develop the original PIV credential validation infrastructure. Since CIV credentials conform to the technical standards of the PIV-I credentials, PIV-I equipment and software should work without changes.

[11] NIST, *Interfaces for Personal Identity Verification* (4 Parts), February 2010, http://csrc.nist.gov/publications/PubsSPs.html

10 Reference Material

FIPS PUB 201-2 Federal Information Processing Standards Publication 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors DRAFT, NIST, March 2011, http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf

HSPD-12 PIV-I Frequently Asked Questions, http://www.va.gov/PIVPROJECT/faq.asp

NIST SP 800-63 *Electronic Authentication Guideline*, April 2006, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

NIST SP 800-73-3 *Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation*, February 2010, http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf

NIST SP 800-73-3 *Interfaces for Personal Identity Verification – Part 2: End-Point PIV Card Application Card Command*, February 2010, http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART2_piv-card-applic-card-common-interface.pdf

NIST SP 800-73-3 *Interfaces for Personal Identity Verification – Part 3: End-Point PIV Client Application Programming Interface*, February 2010, http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART3_piv-client-applic-programming-interface.pdf

NIST SP800-104 *A Scheme for PIV Visual Card Topography*, June 2007, http://csrc.nist.gov/publications/nistpubs/800-104/SP800-104-June29_2007-final.pdf

Personal Identity Verification Interoperability for Non-Federal Issuers, Federal CIO Council, July 2011, http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf

Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Businesses, Smart Card Alliance white paper, February 2011, http://www.smartcardalliance.org/resources/lib/PIV-I_White_Paper_012811.pdf

RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace, http://www.ietf.org/rfc/rfc4122.txt