



**Smart Card
Alliance**

***Personal Identity Verification Interoperability
(PIV-I) for Non-Federal Issuers: Trusted
Identities for Citizens across States, Counties,
Cities and Businesses***

*A Smart Card Alliance Physical Access Council and Identity Council White
Paper*

Publication Date: January 2011

Publication Number: PAC-11001

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>.

Copyright © 2011 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

TABLE OF CONTENTS

1	INTRODUCTION	4
1.1	IDENTITY CREDENTIALS: THE MOVE TOWARD PIV-I	4
2	FOUNDATIONS FOR CREDENTIAL INTEROPERABILITY	6
2.1	POLICY	6
2.1.1	<i>Uniform Electronic Transaction Act</i>	6
2.1.2	<i>Deficit Reduction Act</i>	6
2.1.3	<i>REAL ID Act and Western Hemisphere Travel Initiative</i>	6
2.1.4	<i>U.S. Drug Enforcement Agency’s Rules for Electronically Prescribing Controlled Substances</i>	7
2.1.5	<i>Draft National Strategy for Trusted Identities in Cyberspace</i>	7
2.2	PROCESS	7
2.3	TECHNOLOGY	8
2.3.1	<i>PKI and Trust</i>	8
2.3.2	<i>Smart Card Technology</i>	9
2.3.3	<i>Biometrics and Smart Card Technology</i>	10
2.3.4	<i>PIV-I and PIV-C</i>	10
3	BUSINESS JUSTIFICATION	12
3.1	ADVANTAGES OF ADOPTING FIPS 201	12
3.2	EXAMPLES	12
3.2.1	<i>National Cancer Institute</i>	12
3.2.2	<i>Transglobal Secure Collaboration Program</i>	13
3.2.3	<i>Department of Agriculture</i>	13
3.2.4	<i>State of Illinois</i>	13
3.2.5	<i>GSA</i>	13
3.2.6	<i>Other Ongoing Efforts</i>	14
3.3	SUMMARY	14
4	STATE PROGRAMS	15
5	CONSIDERATIONS FOR FUTURE DIRECTIONS	18
5.1	OTHER FORM FACTORS USING SMART CARD TECHNOLOGY	18
5.2	SMART CARD TECHNOLOGY AND APPLICATIONS	19
6	CONCLUSIONS	20
6.1	POLICY	20
6.2	PROCESS	20
6.3	TECHNOLOGY	20
6.4	SUMMARY	20
7	REFERENCES	21
8	PUBLICATION ACKNOWLEDGEMENTS	22
9	APPENDIX A: STANDARDS EFFORTS	24

1 Introduction

Solid identity management and strong credentialing practices are critical to government organizations and enterprises that must verify the identities of a wide variety of individuals—employees, business partners, emergency response officials, and citizens. As a result governments around the world are putting in place the legal framework to leverage strong identity credentials for eGovernment, eHealth and eCommerce and use of these credentials is growing. This brief talks about the progress in the United States in establishing a standard for identity and credentialing and the associated and necessary trust framework.

Driven by the issuance of Homeland Security Presidential Directive 12 (HSPD-12) in 2004, the U.S. Federal Government has invested significant effort and resources in implementing robust, interoperable credentialing processes and technologies. The resulting standard, *Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors*, provides a framework of the policies, processes, and technology required to establish a strong, comprehensive program. And in fact, since 2005, the Federal Government has successfully used this framework to issue over 5 million PIV cards to Federal employees and contractors. In addition, Federal agencies have developed an infrastructure for using these interoperable credentials to support additional requisite functions, including the following:

- Physical security, including facility access and video analytics
- Logical security, including network and application access
- Incident monitoring and response
- Encryption and protection of sensitive data

State and local governments and other organizations can leverage the Federal program. Two publications—*Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers*¹ (issued by the Federal CIO Council in May 2009) and *PIV-I Frequently Asked Questions*²— provide states, local jurisdictions, and commercial organizations with applicable standards and guidance. The definition of PIV interoperability builds on the Federal PIV standard and the supporting framework of policies, processes, and technologies. The maturity of the Federal standards, the availability of compliant commercial off-the-shelf (COTS) products, and the ability to use a single, interoperable, and secure PIV credential across multiple application areas can enable states, local jurisdictions, and enterprises to improve their security postures, infrastructures, and services for employees, contractors, businesses, and consumers. Using the PIV-I standards helps to provide a foundation for a cost-effective approach.

1.1 Identity Credentials: The Move toward PIV-I

Many state and local organizations point to the PIV standard as a way to achieve a more holistic approach to issuing identity credentials, and improving their own business processes, notwithstanding the additional requirements of implementing supporting infrastructure and applications. More than 16 states are currently planning or implementing some form of PIV-interoperable (PIV-I) or PIV-compatible (PIV-C) strategy. Early state adoption of PIV-I credentials and infrastructure in the Commonwealth of Virginia, the State of Colorado, and the State of Illinois has established baselines for achieving interoperability with Federal credentials, services, and systems. These PIV-I credentials are being used in regional and national interoperability exercises sponsored by the Federal Emergency Management Agency (FEMA)³

¹ "Personal Identity Verification Interoperability for Non-Federal Issuers," Version 1.1, Federal CIO Council, July 2010, http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf

² "Personal Identity Verification Interoperable (PIV-I): Frequently Asked Questions (FAQ)," Version 1.0, CIO Council, June 28, 2010, http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf

³ "Spring Ahead: Federal and Mutual Aid Emergency Response Official Electronic Credentialing and Validation Interoperability Demonstration - May 19, 21, 2009," FEMA After Action Report,

and for piloting operations in other areas, such as accessing Federal systems. In the July 2010 white paper, *Moving towards Credentialing Interoperability: Case Studies at the State, Local and Regional Level*,⁴ seven states highlighted ongoing and planned activities for deploying PIV-I credentials within their jurisdictions.

During the April 2010 National Association of State Chief Information Officers (NASCIO) Digital Identity Workshop⁵, a working group was established to put together a charter for a NASCIO Digital Identity Working Group. Many states and jurisdictions already use components of PIV-I policy or process, such as strong identity vetting procedures, public key infrastructure (PKI), and smart cards, within their enterprises. These existing components can be leveraged to establish interoperable digital identities.

This white paper suggests that NASCIO recommend and advocate standards, policies, and technology based on the PIV-I guidance established by the Federal Government. The identity, credentialing, and access management (ICAM) guidance and roadmap⁶ that accompany the PIV standard and PIV-I guidance provide states with a process for this effort. The identity credentials issued by states can be made more widely applicable, be used more efficiently, and enhance citizen privacy when used to support state privacy legislation and policies and state initiatives to protect citizen personal information. States can move from issuing multiple credentials for a variety of state programs to issuing a single, multi-purpose, trusted PIV-I credential.

Education is key to enabling state and local governments to appreciate the industry-wide investment in, experience with, and benefits of current PIV and PIV-I deployments and solutions. Such education includes highlighting ongoing developments in both public and private enterprises and the availability of over 500 PIV-compliant products currently on the General Services Administration (GSA) Approved Products List⁷.

This white paper is intended to help state and local jurisdictions explore the following issues:

- The policies, processes, and technologies available to achieve interoperability
- The value of a single multi-purpose credential, including cost, security, and privacy benefits
- What state programs are suitable candidates for considering a move to an interoperable identity credential
- Future considerations for technology migration

<http://www.dps.mo.gov/HomelandSecurity/documents/Credentialing/Spring%20Ahead%20AAR%20July%202009.pdf>

⁴ http://www.safecomprogram.gov/NR/rdonlyres/648C73A5-022C-4E1E-84EB-8DFEFCA0C382/0/2aMovingTowardsCredentialingInteroperability_7810.pdf

⁵ <http://www.nascio.org/committees/digitalID/>

⁶ "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance," Federal CIO Council, November 10, 2009,

http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

⁷ <http://fips201ep.cio.gov/apl.php>

2 Foundations for Credential Interoperability

Creating interoperable identity credentials requires consideration of guidance policies, identity vetting and verification processes, and credentialing technology.

2.1 Policy

Current state identity and credential policies are typically designed to apply to specific use cases. That is, states issue driver's licenses to authorize driving, fishing licenses for fishing, and hunting licenses for hunting; business and medical credentials follow the same approach.

However, new policies, technology innovations, and current standards development and processes can support a different approach to identity and credentialing. New state policies required by the following national directives can be aligned with strong interoperable identity standards and PIV-I:

- Uniform Electronic Transaction Act
- Deficit Reduction Act
- REAL ID Act and Western Hemisphere Travel Initiative
- U.S. Drug Enforcement Agency's rules for electronically prescribing controlled substances
- Draft National Strategy for Trusted Identities in Cyberspace

Formulation of a common identity credential approach that addresses these policies can provide an opportunity for state executives to enact or ratify standards and deploy resources and infrastructure to achieve outcomes that are reusable across the state's identity management programs. Resources can be focused on improving outcomes for citizens, businesses, universities, healthcare providers, and governmental entities at all levels.

2.1.1 Uniform Electronic Transaction Act

The Uniform Electronic Transaction Act (UETA) was put in final draft form in 1999.⁸ A total of 47 states have since enacted portions of the UETA into law. The Act facilitates and authorizes the use of electronic records and electronic signatures. The legal framework for UETA provides for digital signatures, electronic forms, and other electronic business applications. Several states with PKI programs have instituted procedures to convert this policy into practice. The policy in some jurisdictions gives executives the authority to approve standards to implement UETA.

2.1.2 Deficit Reduction Act

In the Deficit Reduction Act of 2005, the Centers for Medicare and Medicaid Services (CMS) were given the mandate to establish the identity, citizenship and entitlement for all beneficiaries and providers.

2.1.3 REAL ID Act and Western Hemisphere Travel Initiative

The REAL ID Act regulates standards for identity proofing that supports trust between citizens, states, and the Federal Government. The Western Hemisphere Travel Initiative (WHTI)⁹ requires specific documents when entering the United States that will enable the Department of Homeland Security (DHS) to quickly and reliably identify a traveler. States that issue Enhanced Driver Licenses (EDLs) or Enhanced Identification Credentials (EIDs) work together with DHS to set requirements for the issuance of these documents.

⁸ <http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm>

⁹ http://travel.state.gov/travel/cbpmc/cbpmc_2223.html

Many states are implementing identity programs under these programs using common identity proofing standards and practices.

2.1.4 U.S. Drug Enforcement Agency's Rules for Electronically Prescribing Controlled Substances

On March 24, 2010, the DEA published an interim final rule (IFF) in The Federal Register. In the new regulation, users of e-prescribing systems for controlled substances would prove their identities with two of the following three factors: something you know (password); something you have (token); something you are (biometric).

The IFF states, "Authentication based only on knowledge factors is easily subverted because they can be observed, guessed, or hacked and used without the practitioner's knowledge. In the interim final rule DEA is allowing the use of a biometric as a substitute for a hard token or a password."¹⁰

As a very high assurance identity credential, PIV-I meets and exceeds the authentication requirements mandated by the DEA.

2.1.5 Draft National Strategy for Trusted Identities in Cyberspace

The Draft National Strategy for Trusted Identities in Cyberspace (NSTIC), which is still under development, provides a policy framework by describing a comprehensive identity ecosystem. The strategy includes implementing an interoperable identity for citizens for personal and professional use, including e-mail messages, banking, and access to health information. The strategy can be extended to protect devices and infrastructure, such as the devices included in and the infrastructure underlying a so-called "smart grid." The strategy envisions a scenario in which an identity issued in one state can be used to access information locally, regionally, or nationally and can be trusted by public and private enterprises. An extract from the NSTIC "Executive Summary" clearly identifies the need for a comprehensive strategy for strong identities:

One key step in reducing online fraud and identity theft is to increase the level of trust associated with identities in cyberspace. While this Strategy recognizes the value of anonymity for many online transactions (e.g., blog postings), for other types of transactions (e.g., online banking or accessing electronic health records) it is important that the parties to that transaction have a high degree of trust that they are interacting with known entities. Spoofed websites, stolen passwords, and compromised login accounts are all symptoms of an untrustworthy computing environment. This Strategy seeks to identify ways to raise the level of trust associated with the identities of individuals, organizations, services, and devices involved in certain types of online transactions.¹¹

The NSTIC provides an opportunity for states to leverage PIV and PIV-I credential definitions and the associated trust framework to enable enhanced security and privacy, implement strong identity policy and support open standards.

2.2 Process

States have for some time provided credentials that are trusted outside of their domains, in the form of a driver's license. However, these credentials were never intended to support additional use cases such as access to cyberspace, physical resources, or incident scenes.

This situation is beginning to change. There are now standards for international electronic driver's licenses and identity credentials, and hundreds of millions of credentials have been issued that meet these standards. In the United States, REAL ID, WHTI and FIPS 201 programs

¹⁰ U.S. Dept. of Justice, Drug Enforcement Administration, "Electronic Prescriptions for Controlled Substances," 21 CFR Parts 1300, 1304, 1306, 1311, Federal Register notice, Docket No. DEA-2181, RIN 1117-AA61, March 24, 2010, page 27.

¹¹ "Draft National Strategy for Trusted Identities in Cyberspace," June 25, 2010, http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

are examples of standards for identity credentialing efforts that are being implemented at the national and state level. The combination of FIPS 201 with other standards and specifications developed by international standards-setting bodies and commercial associations¹² can provide an overall solution for identity credentialing effort. States are increasingly issuing trusted electronic identity credentials that meet these standards. States can put into place processes based on standards that enable trust and strong electronic authentication and validation outside of their jurisdictions, increasing the value and use of these credentials in the process.

For example, Michigan, New York, Vermont, and Washington State are leading the WHTI standards implementation effort and are using complying identity credentials for both state identification and for Canadian border crossings in lieu of a passport. Other states, such as Virginia, Colorado, and Pennsylvania, are issuing PIV-I identity credentials that comply with the identity proofing and vetting standards specified in NIST SP-800-63, *Electronic Authentication Guidance*.¹³ These PIV-I identity credentials are used predominantly at incident scenes as first responder credentials, but the credentials can also be used for digital signatures and other functions requiring strong electronic authentication.

CIOs and their CISOs can take advantage of the PIV-I standard. The standard clearly defines the process steps, roles, and responsibilities required to issue a high assurance, multi-purpose electronic identity credential. The standards-based technology used by the credentials ensures the establishment of security, privacy, and trust, promoting interoperability.

2.3 Technology

Technical interoperability of credentials depends on strong and stable standards. The PIV and PIV-I technology and infrastructure are based on standards at many levels – from the physical token (the smart card) to the identity credential components to the PKI that enables interoperable trust. PIV and PIV-I are based on FIPS 201 and accompanying special publications, and reference other internationally recognized standards. The General Services Administration operates independent testing procedures to validate and approve products that comply with FIPS 201 and publishes the results as an Approved Products List (APL).

PIV-I credentials provide secure, multi-factor authentication at the high level of assurance required. PIV-I combines a modern and mathematically strong authentication factor (the cryptographic private key) with a personal identification number (PIN), fingerprint biometric template, and tamper-proof digital photograph. This combination provides high assurance levels, allows the cardholder to control the release of information, and provides a trusted identity that can be used for a wide range of cyber and physical transactions.

2.3.1 PKI and Trust

A federated identity infrastructure imposes obligations among parties involved to establish contractual agreements. These agreements address issues related to policies and procedures in order to achieve a high level of assurance, trust and interoperability, such as can be provided by a cross-certified public key infrastructure as used with PIV-I.

A PKI is the architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Also included in a PKI are the certificate policies and agreements among parties that document the operating rules, procedural policies, and liabilities of the parties operating within the PKI.

A PKI provides the foundation for interoperable trust. The basis for the trust is the digital certificate issued by a trusted third party, the certificate authority (CA). A digital certificate binds

¹² For example, the International Civil Aviation Organization (ICAO), the American National Standards Institute (ANSI), the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF), among others.

¹³ "Electronic Authentication Guidance," NIST SP 800-63, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

an asymmetric public key to identity information under a particular PKI policy. Individuals use the digital certificates in transactions. When a individual digitally signs a transaction using the certificate, the relying party can verify the individual's signature and query the CA to ensure that the certificate is valid. If both are valid, the relying party can trust that the individual signing the message is who they say they are.

The Federal Bridge Certificate Authority (FBCA)¹⁴ was established by the Federal Government to extend trust across all Federal agencies and is the chief mechanism for enabling trust between industry (external) PKI implementations and Federal (internal) PKI implementations. The FBCA has also established trust relationships with sister certificate authorities, including authorities in the biopharmaceutical industry, the aerospace and defense industry, the higher education community,¹⁵ and some early adopter states. The establishment of this framework took many years, and it can be leveraged to extend trust across the nation. Cross-certification can allow Federal agencies and external organizations to trust each others' PKI certificates and enable interoperable trusted transactions. Currently, external partners associated with the FBCA include one state (Illinois) and two industry PKI bridges (CertiPath for the aerospace and defense industry and SAFE-BioPharma for the pharmaceutical and healthcare industries).

2.3.2 Smart Card Technology

A decision critical to the security of an identity system is the selection of an identification (ID) technology. Many current ID or badging systems rely on technologies such as magnetic stripes or bar codes. These technologies cannot fulfill the requirement to provide strong security while still guarding privacy. IDs based on these technologies are tamper-prone, can be counterfeited easily, and provide little or no protection for the information they carry.

IDs that use smart card technology have the security features required to enhance privacy protection in a well-designed and properly implemented system. Smart card technology incorporates a small computer chip in a card (or other form factor). The embedded chip provides smart cards with built-in tamper resistance and the unique ability to store large amounts of data securely, carry out functions on the card itself, and interact intelligently with a smart card reader.

Smart card technology therefore provides an identity management system with strong information and privacy protection, strong ID security, sophisticated "on-card" processing (encryption, decryption, biometric matching), and authenticated and authorized information access. Implemented properly, smart card technology strengthens the ability of any organization to protect the privacy of individuals whose identity the organization must verify. Unlike other IDs, smart card-based IDs can implement a personal "firewall," releasing only required information and only when it is genuinely required, making them excellent guardians of personal information and individual privacy. Smart cards can be used readily online and across networks and deliver very high levels of security over the Internet. They are also convenient and easy to use.

PIV-I credentials are based on secure, microprocessor-based smart card technology. The credentials include a dual-interface integrated circuit (or chip) that allows both contact and contactless operations. This capability allows a PIV-I credential to take a number of forms, such as a plastic smart card, a USB token, or a smart phone. It also allows PIV-I credentials to be included in a wide variety of devices.

Over 5 billion smart cards are shipped annually.¹⁶ The financial payments industry has moved to smart cards, with the majority of regional financial organizations worldwide mandating the use of smart cards as financial credit and debit cards by a specific date. Smart card-based healthcare ID cards are also issued in many countries; France and Germany, for example, have issued over 140 million smart healthcare ID cards to their citizens. Smart card technology is also built into every GSM mobile phone's subscriber identity module (SIM).

¹⁴ For additional information on the Federal Bridge Certificate Authority, see <http://www.idmanagement.gov/fpkia/>

¹⁵ <http://www.the4bf.com/>

¹⁶ Source: Eurosmart, <http://www.eurosmart.com/>

All smart card initiatives are based on a set of global standards. Adopting smart card technology and the PIV standards provides a low-risk, highly secure, multi-use credential for state and local governments. Using smart cards, organizations can implement a layered security architecture that addresses expected security risks and incorporates an end-to-end chain of trust.

2.3.3 Biometrics and Smart Card Technology

Biometric technology can provide a very high level of assurance for confirming an enrolled individual's identity when used in conjunction with a smart card. Examples of biometric data include fingerprints, iris patterns, facial images, and vein patterns. One or more biometric samples can be registered when an individual's identity is initially vetted and enrolled for an identity credential. The biometric data used for subsequent matching, called a template, is created using the original biometric data. The template is stored in a reduced digital format and consists of only those features needed for the matching process, which are extracted from the original data. The template enhances privacy, since it cannot be easily reconstructed into the original image.

Smart card-based identity credentials can securely store biometric information, and the card can compare that information with a presented biometric to verify an individual's identity. This capability enhances privacy: the individual's stored biometric information never leaves the ID card (which remains in the individual's possession) and the stored biometric can be compared to the presented biometric within the reader, host computer or even within the smart card chip's secure processing environment.

Biometrics can be used in a wide variety of applications (see Table 1) as a second or third factor of authentication, providing stronger assurance that an individual's identity is accurately verified.

Table 1. Applications and Features for Biometrics

Applications	Features
Transaction authentication	Always with you
Physical access control	Convenient
Secure logon	Easy to use
Biometric Social Security	Low cost
Entitlement program ID	
E-payment	
E-signature	
E-ticketing	
E-voting	

2.3.4 PIV-I and PIV-C

Non-federal issuers of identity cards have expressed a desire to issue identity cards that are trusted by Federal Government relying parties and can interoperate with Federal Government PIV systems. The Federal CIO Council published a guidance document, *Personal Identity Verification Interoperability for Non-Federal Issuers*, in May 2009.¹⁷ This document includes a minimum set of requirements that describes how such an identity card can technically interoperate with Federal Government PIV systems and be trusted by Federal Government relying parties. The document defines three cards:

- PIV card
- PIV interoperable (PIV-I) card
- PIV compatible (PIV-C) card

¹⁷ "Personal Identity Verification Interoperability for Non-Federal Issuers," Federal CIO Council, May 2009 and July 2010, http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf

The PIV card is an identity card that conforms fully to Federal PIV standards. Only cards issued by Federal entities can fully conform. Federal standards ensure that PIV cards are interoperable with and trusted by all Federal Government relying parties.

The PIV-I card is an identity card that meets the PIV technical specifications, works with PIV infrastructure elements, such as card readers, and is issued in a manner that allows Federal Government relying parties to trust the card.

The PIV-C card is an identity card that meets the PIV technical specifications: the card can work with PIV infrastructure elements, such as card readers, but the card itself has not necessarily been issued in a manner that assures it is trustworthy by Federal Government relying parties.

A state or local government can choose to implement a PIV-I or a PIV-C card. A PIV-I card builds on the PIV-C card, with the issuer procuring a PIV-C card and issuing it in a manner consistent with FIPS 201 policies and processes. The PIV-I card can then be trusted by both the state or local government and the Federal Government.

While a PIV-C card would not be trusted by Federal Government relying parties, it would be technically compatible with PIV infrastructure elements, such as card readers. Authorities issuing either a PIV-I or PIV-C card could therefore take advantage of the growing number of approved products that are available to support the PIV infrastructure.

3 Business Justification

Coordinating multiple independent credentialing and identity management efforts can be a challenge. It is challenging enough to manage identities and attributes locally, and even more challenging to manage them when dealing with multi-jurisdictional interoperability. Credentialing and identity management solutions are particularly costly when implementation is not based on standards and best practices.

3.1 Advantages of Adopting FIPS 201

The adoption of FIPS 201 as the basis for issuing a PIV-I or PIV-C card can substantially reduce these challenges. Adoption can:

- Provide interoperability across multiple jurisdictions
Adoption of FIPS 201 will reduce redundant credentialing efforts and expenditures, allow one ID to be issued (rather than multiple IDs), and increase policy effectiveness.
- Provide trust across multiple jurisdictions
Adoption of FIPS 201 will implement a standardized identity proofing process and standardized issuance procedures.
- Provide strong proof of cardholder identity
FIPS 201 enables processes that maintain and protect data from accidental or deliberate loss, alteration, or destruction. Data accuracy is enhanced through processes that prevent, detect, and correct errors.
- Provide the ability to authenticate identity and attributes electronically
Electronic authentication enhances data security, physical security, and personal privacy while allowing for secure physical and logical access. It also protects against identity theft and reduces the incidence of fraudulent benefit, entitlement, or service payments to individuals who misrepresent themselves.
- Improve ROI for identity credentialing programs
The ability to leverage a common identity infrastructure and technology across multiple credentialing programs can improve return on investment. In addition, the GSA co-op purchasing program is available to state and local governments so that they can acquire products through a GSA purchasing vehicle¹⁸. For first responder credentialing programs, the U.S. Department of Homeland Security has potential grant funding available.

FIPS 201 leverages existing ANSI, ISO, IETF and other standards. Thousands of products including most operating systems, mobile and enterprise applications and services and physical access control system support PIV-I credentials because of these standards.

3.2 Examples

Organizations that have implemented PIV and other strong authentication credentials and established the associated infrastructure have experienced improved business processes, as described in the examples below. Organizations that adopt PIV-I credentials can take advantage of high-assurance, trusted relying-party infrastructures.

3.2.1 National Cancer Institute

Use of strong authentication credentials and the Federal Bridge trust model has enabled the National Cancer Institute and the laboratories and pharmaceutical and medical companies involved in cancer research to achieve an overall cost savings of more than \$40,000 per 100 people, by converting paper

¹⁸ GSA Advantage: https://www.gsaadvantage.gov/advgsa/advantage/main/start_page.do; Coop Purchasing: <http://www.gsa.gov/portal/content/104449>

documents to electronically signed documents.¹⁹ This example illustrates what can happen when identity credential users and electronic transaction capabilities work together.

3.2.2 Transglobal Secure Collaboration Program

The Transglobal Secure Collaboration Program (TSCP) is a cooperative forum in which leading aerospace and defense (A&D) companies, key government agencies and technology companies work together to define open specifications and common operating rules that can be used to enable secure collaboration and assured information sharing between organizations, irrespective of the tools they choose to use. Each TSCP member company/organization has (or will establish) a PKI which is cross-certified with CertiPath. Personnel in these organizations use their PIV or PIV-I certificates to send signed and encrypted email as well as enable federated access to information held on external systems. In 2008, TSCP drove the U.S. Department of Defense memorandum of understanding for approval of external public key infrastructures.

3.2.3 Department of Agriculture

The United States Department of Agriculture (USDA)²⁰ investment in identity proofing and credential issuance is realizing benefits across the department in the form of consolidated access management. USDA has reported that the agency benefits include: trusting credentials issued by third parties within their identity credentialing and access management (ICAM)²¹ architecture; automatically provisioning access roles and reducing the need for staff to do manual provisioning; and streamlining business processes.

3.2.4 State of Illinois

As an early adopter of PKI credentials cross-certified to the Federal Bridge, the State of Illinois²² is leveraging the UETA to enable trusted digital signatures and access in over 40 state agencies and universities. Illinois citizens and businesses are presently being enrolled at a rate of 600–800 entities per month. The state will realize more efficient business processes that will result in cost savings, as citizens use their credentials to authenticate to systems, sign documents and electronic forms digitally, and encrypt and sign e-mail messages.

3.2.5 GSA

GSA presented their ICAM implementation achievements during the June 2010 Government Smart Card Interagency Advisory Board²³ meeting and were featured in the August *Federal Computer Weekly*²⁴ as part of other GSA CIO accomplishments. GSA set new records by enabling 90 percent of personnel to use their PIV credentials for workstation logon in less than 90 days from project initiation.

¹⁹ "Research Collaboration in the Cloud: How NCI and Research Partners Are Improving Business Processes Using Digital Identities," http://www.fips201.com/resources/audio/iab_0710/iab_072810_ansher_and_cullen.pdf

²⁰ "ICAM Progress at USDA," Owen Unangst, USDA, presentation, Smart Card Interagency Advisory Board (IAB) meeting, May 27, 2010, http://www.fips201.com/resources/audio/iab_0510/iab_052710_unangst.pdf, http://www.fips201.com/resources/audio/iab_0510/iab_052710_spencer.mp3

²¹ Identity, Credential and Access Management (ICAM): The goal is a [consolidated](#) approach for all government-wide identity, credential and access management activities to ensure alignment, clarity, and interoperability, <http://www.idmanagement.gov>

²² "The Realized Value of the Federal Public Key Infrastructure (FPKI), Identity Credential and Access Management Subcommittee, Jan. 29, 2010, <http://www.idmanagement.gov/documents/RealizedValueFederalPKI.pdf>

²³ "Update on GSA's ICAM Implementation to the Smartcard IAB," Bill Erwin, GSA, presentation, Smart Card Interagency Advisory Board (IAB) meeting, June 29, 2010, http://www.fips201.com/resources/audio/iab_0610/iab_062910_erwin.pdf

²⁴ "How to fast-track IT modernization projects," Federal Computer Week, August 9, 2010, <http://fcw.com/articles/2010/08/23/comment-casey-coleman-gsa-slam-modernization.aspx>

3.2.6 Other Ongoing Efforts

DHS and the Federal Emergency Management Agency (FEMA) have been working with many states on deploying First Responder Authentication Credentials (FRAC), leveraging the PIV-I framework. Among the states, Virginia, Texas, Pennsylvania, Colorado, West Virginia, Hawaii and the District of Columbia have reported significant benefits as a result of their activities.²⁵

In late 2009, the Command, Control and Interoperability (CCI) Division within the Science & Technology (S&T) Directorate, the FEMA Office of National Capital Region Coordination (NCRC), and the FEMA Office of Security (OS) partnered to convene the PIV-I/FRAC Technology Transition Working Group (TTWG). The TTWG is composed of state and local emergency management representatives, many of whom have already implemented innovative and secure identity management solutions in their own jurisdictions. Local and state participants in the work group include Colorado, Maryland, Virginia, District of Columbia, Missouri, Southwest Texas, Pennsylvania, West Virginia, Hawaii, and Illinois. The working group is focused on exploring PIV-I credentials as the standard that will enable interoperability between local and state emergency response officials.²⁶

3.3 Summary

The adoption of interoperable credential technology and infrastructure by such industry groups as the aerospace and defense and the biopharmaceutical industries and by Federal and state agencies is expanding the deployed based of interoperable products. Broader PIV-I adoption will move the infrastructure toward a tipping point where the standards-based solution has significant benefits over non-standards-based approaches. Most businesses, states, counties, and cities are still supporting hundreds of legacy identity solutions that were developed to support limited-use applications or networked users. Continuing to support such identity and authentication solutions incurs operational costs and adds little or no value for the taxpayers served by these systems.

With the time required for implementation decreasing and number of readily available products and services increasing, state, county, and city officials as well as business leaders can easily leverage the Federal Government's work on PIV. Following the path blazed by the Federal Government and early adopters by implementing a standards-based PIV credential can result in successful credentialing and identity management solutions that reduce the challenges of managing identities and attributes.

²⁵ "Moving towards Credentialing Interoperability: Case Studies at the State, Local and Regional Level," U.S. Department of Homeland Security, July 2010²⁵

²⁶ PIV-I/FRAC Technology Transition Working Group, U.S. Department of Homeland Security Command, Control and Interoperability Division

4 State Programs

As states are faced with increasing challenges of deploying comprehensive strategies to comply with national strategies, the ability to leverage existing state programs that require identity management is imperative. State organizations are sensitive to expenses and are looking for a return on their investment. States have implemented or are planning policies and programs that can be leveraged to achieve a comprehensive and rich identity ecosystem. These programs include:

- Enterprise identity and access management
- Cloud computing
- Healthcare information exchange frameworks
- Emergency response activities
- Entitlement programs
- Digital records management

A common theme throughout the existing state use cases for PIV-I has been the ability to use credentials for multiple applications, from physicians to emergency response to desktop logon to digital signatures. Table 2 lists policy, process, and technology considerations that the Smart Card Alliance considers germane to state identity programs, which are complex and may often be organized across program areas. For each consideration, the table identifies high level gaps and suggests how to close each gap and transition to a unified and standards-based approach.

Table 2. Considerations for State Activities

Existing Program or Policy	Gap	Suggested Strategy
Uniform Electronic Transactions Act	While the legal framework for UETA provides for digital signatures, electronic forms, and other electronic business applications, a policy may not be in place to deploy legally binding digital transactions effectively.	As part of programs to reduce paperwork and transition to online citizen-centric services, allow for strong digital signatures to be used in conjunction with a high assurance identity credential such as PIV-I.
Electronic Signatures in Global and National Commerce Act (E-Sign Act of 2000)	The act establishes the ability to accept electronic signatures as legally viable but does not establish a common framework that allows organizations to trust digital signature processes and technologies across organizational boundaries.	Establish state policy that leverages the policies used by the FBCA, the Four Bridges Forum (4BF), and the European Union to allow for digital signatures which leverage the PIV-I credential to be accepted and trusted.
State policies and acceptance of PIV and PIV-I credentials	Most state-run programs currently accepting digital identities for strong authentication and digital signatures do not accept externally issued credentials such as PIV and PIV-I.	Assess the PIV and PIV-I policies established by the Federal Government and modify state or agency policies to accept these credentials.
First Responder Authentication Credential (FRAC) programs	Ability to leverage FRAC/PIV-I credentials for electronic commerce, digital signatures, and other state and consumer programs requires collaboration across multiple agencies.	Assess current state policies for use of digital identities and incorporate stakeholder buy-in at the state CIO level to use PIV-I credentials for additional applications.

Existing Program or Policy	Gap	Suggested Strategy
Drug Enforcement Agency's March 25, 2010 Interim Final Rule for electronically prescribing controlled substances	A user name and password combination for identity verification is not strong enough to authenticate prescribing physicians to the required software applications.	PIV-I credentials meet the two-factor authentication requirements of this rule. An assessment of PIV-I and its acceptance should be included in any health information exchange (HIE) and ePrescribing framework.
WHTI and REAL ID identity authentication	Neither the WHTI nor REAL ID credential require use of biometrics for stronger two-factor authentication and verification of identity. The use of biometric data (e.g., fingerprints, facial or iris) provides a foundation for achieving three-factor authentication for high risk transactions (physical or logical access). Lack of biometric data or another "what you are" factor prevents credentials from being leveraged in the PIV-I trust framework.	Offer consumers the ability to opt-in and add biometrics to their credentials during the identity verification and issuance process, for use in high assurance identity authentication.
Establishment of an individual's digital identity	Not all programs in use or in process check identities against a centralized authority or allow for in-person identity proofing.	Provide a mechanism for individuals and business signing authorities to opt-in and perform in-person identity proofing to move towards a higher assurance credential such as PIV-I.
Mandatory requirements for governance and compliance, including Sarbanes-Oxley, HIPAA, NERC-CIP, and PCI DSS	Security, privacy, and auditability are foundations of common governance and compliance regulations. However, organizations may not currently implement compliance programs in unison across the organization.	Leveraging a PIV-I framework and ICAM-like processes can help organizations meet these requirements. Adopting a unified framework can help provide stronger controls and decrease inefficiencies and costs.
State-run PKIs	State-run PKIs may not leverage a common policy for issuance and maintenance that allows for trust to be established across organization and state boundaries.	<p>For those states with more mature PKI infrastructures, assess the state certificate policies and map them to the policies used by the FBCA and the 4BF. Consider necessary modifications and initiate procedures to cross-certify.</p> <p>For those states with minimal reusable PKI infrastructures, leverage the FBCA and 4BF infrastructures already in place for efficiency and cost savings.</p> <p>Consider leveraging the existing PIV-I policy²⁷, technology and process to generate and carry the certificates to achieve medium assurance hardware-based credentials.</p>

²⁷ "Citizen and Commerce Class Certificate Policy, Version 2.2, Federal Public Key Infrastructure Policy Authority, August 25, 2010, http://www.idmanagement.gov/fpkipa/documents/citizen_commerce_cp.pdf

Existing Program or Policy	Gap	Suggested Strategy
Form factors used to store digital identity certificates	Storage of digital identity credentials may be in form factors that are not as tamper-resistant or portable as PIV-I or other smart card tokens.	For programs requiring high assurance identity authentication, the PIV-I and PIV-C credential provides strong token security.
State system acceptance of PIV and PIV-I credentials and migration to cloud computing environments	State-run systems currently accepting digital identities for strong authentication and digital signatures do not accept third-party trusted credentials such as PIV and PIV-I.	<p>Enable applications to accept digital certificates carried on the PIV and PIV-I credentials issued by organizations external to the state.</p> <p>Ensure that migration strategies for cloud computing include a comprehensive analysis of authentication frameworks and leverage the PIV-I credentials.</p>

5 Considerations for Future Directions

States are currently in the process of implementing their own complementary programs for identity credentialing, developing a comprehensive framework or approach, and evaluating how these can leverage the Federal PIV infrastructure. Integral to this process are identifying the highest value areas for first implementation to improve trust and provide proof of concept, identifying areas (if applicable) where a dense population of Federal PIV credentials exists, and modifying services to leverage these credentials.

This section highlights technology, application and use case considerations that can build on the investment in the PIV-I credential and infrastructure, add value for state government, and further strengthen authentication processes.

5.1 Other Form Factors Using Smart Card Technology

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

Each form factor provides a different set of features and benefits and can support a variety of applications. Table 3 lists the unique features and requirements for different form factors.

Table 3. Users, Applications, and Features for Available Credential Form Factors

Form Factor	Users	Applications	Features
Smart card	General public Government agencies DoD Students First responders: police, fire, medical, utility, communications Transportation workers: aviation, maritime, railway, bus transit, taxi Office workers Legal services	Secure driver's license Biometric Social Security Entitlement program identification Travel identity (e-passport) Biometric authentication Secure logon Transit pass E-payment Physical access control E-signature E-ticketing E-voting E-mail encryption	Contactless or contact Challenge/response security Data encryption Stored biometrics template Multi-factor authentication (card + PIN, card + biometric, card + picture, card + PIN + biometric) Stored certificates Basic data processing Biometrics (match-on-card) Low cost
NFC-enabled smart phone ²⁸	Students First responders: police, fire, medical, utility, communications General public Office workers Bus transit Taxi Legal services	Biometric authentication Automatic location sensing (GPS) Signed certificates Encryption key, source/compute Physical access control E-payment E-signature E-ticketing E-voting E-directions Secure data exchange Browser capability	Contactless Convenient Color display Battery powered Powerful CPU functions Advanced computing power Security (challenge/response) Data encryption Data processing Multi-factor authentication Biometrics (match-on-board) SMS—specific text

²⁸ Additional information on NFC can be found on the NFC Forum web site, <http://www.nfc-forum.org>

Form Factor	Users	Applications	Features
		E-mail encryption	Tweet—broadcast Information Bluetooth®—device communications User authentication to phone (PIN, biometric) Infrared data port—machine-to-machine (M2M) communications Smart browser (posters, signs)
Car key fob	General driving public	Physical access control E-signature Biometric authentication Transit pass Vehicle key	Contactless Convenient Battery powered Read range Biometric sensor (option) Infrared data port—M2M communications
Digital wristwatch	General public Manufacturing	Physical access control E-ticketing Transit pass Clean environment (e.g., bunny suit) Sports (e.g., ski pass, aquatics)	Contactless Convenient Easy to use Hands-free
USB device	General public Office worker Telecommuter	Secure logon Signed certificates Encryption key, source/compute Encrypt e-mail E-payment E-signature E-ticketing E-voting	Security Powered device Advanced data processing Biometric sensor (option) Direct connect

5.2 Smart Card Technology and Applications

Adoption of identity credentials based on smart card technology creates opportunities for a variety of new applications:

- Use the biometric on the smart credential to authenticate identity
- Get on the bus or subway by tapping the smart credential on the fare box
- Pay for goods with a tap of the smart credential
- Open your office door using the smart credential
- Use the smart credential as an event ticket
- Securely vote anywhere using the smart credential
- Get information by touching the smart credential to smart posters
- Use the smart credential to securely log on to a computer or web site
- Digitally sign a document using the smart credential
- Use the smart credential to encrypt an e-mail message

Smart card technology-based applications can deliver value to governments, businesses, and citizens, including increased convenience, reduced fraud, reduced costs, and improved service delivery.

6 Conclusions

The Smart Card Alliance developed this white paper to provide an educational resource to NASCIO and the NASCIO State Digital Identity Working Group, as they continue their efforts to provide a consensus-based forum to collaborate on developing recommendations on federated identity management initiatives.

The white paper discusses policy, process and technology considerations related to the implementation of state and local government identity credentialing initiatives. The white paper summarizes important aspects of the current state of policy, process and technology and identifies opportunities to support additional work to further improve each through the use of the PIV-I framework and the PIV standard.

As an increasing number of industries and organizations embrace the PIV-I framework for different applications, government and commercial enterprises continue to see increasing product availability and lower costs of deployment and realize the benefits of interoperable trusted credentials.

6.1 Policy

Existing state and Federal policy is sufficient to support a fully successful and robust deployment of a citizen-facing PIV-I implementation by state and local governments and commercial enterprises. This is illustrated by the current initiatives already underway in several states.

The ongoing policy debate will continue to raise the bar on identity vetting and proofing for state- issued identity credentials. State and local governments should consider adopting current standards and best practices. States could establish policy by adopting the PIV-I framework for state-issued identity credentials

6.2 Process

The PIV-I processes defined by the Federal CIO Council in the *Personal Identity Verification Interoperability for Non-Federal Issuers* guidance allow states to begin implementation. Several states are already using the PIV-I framework for their FRAC and other state programs. Shared service providers must meet annual audit requirements measured with a service level agreement in order to maintain their cross-certification to the Federal Bridge. These services can be leveraged and provide the responsibility and liability for a large part of the process.

Many states already meet the adjudication requirements for in-person identity proofing as outlined in the PIV-I framework. Even if states do not currently have the infrastructure to issue a PIV-I credential, a critical first step toward interoperability would be to begin standardizing the in-person identity proofing processes across state programs.

6.3 Technology

The technology to support PIV-I identity credentialing efforts is available and has been proven in both Federal and state implementations. The industry and government investment in PIV and the PIV-I framework has created a clear path for state and local governments and commercial enterprises to improve identity credentialing efforts by using mature standards and interoperable products and processes. PIV-I and the underlying technology is widely supported in many products available from hardware and software vendors today.

6.4 Summary

The Smart Card Alliance has been active in providing guidance and support to government and industry on the use of standards-based strong identity credentials. For over ten years, the Alliance has provided educational resources and guidance for implementing smart card technology in government and commercial identity programs. The Smart Card Alliance has supported the development of the FIPS 201 standard and the associated technical special publications for personal identity verification. The Alliance continues to be involved in the evolution of FIPS 201 and the development of the PIV-I framework for state, local and commercial organizations. The Smart Card Alliance is committed to continue to work with organizations to support the development of PIV-I programs .

7 References

- "Citizen and Commerce Class Certificate Policy, Version 2.2, Federal Public Key Infrastructure Policy Authority, August 25, 2010, http://www.idmanagement.gov/fkipa/documents/citizen_commerce_cp.pdf
- "Draft National Strategy for Trusted Identities in Cyberspace," June 25, 2010, http://www.dhs.gov/xlibrary/assets/ns_tic.pdf
- "Electronic Authentication Guidance," NIST SP 800-63, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance," Federal CIO Council, November 10, 2009, http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf
- "How to fast-track IT modernization projects," Federal Computer Week, August 9, 2010, <http://fcw.com/articles/2010/08/23/comment-casey-coleman-gsa-slam-modernization.aspx>
- "ICAM Progress at USDA," Owen Unangst, USDA, presentation, Smart Card Interagency Advisory Board (IAB) meeting, May 27, 2010, http://www.fips201.com/resources/audio/iab_0510/iab_052710_unangst.pdf, http://www.fips201.com/resources/audio/iab_0510/iab_052710_spencer.mp3
- "Moving towards Credentialing Interoperability: Case Studies at the State, Local and Regional Level," DHS white paper, July 2010, http://www.safecomprogram.gov/NR/ronlyres/648C73A5-022C-4E1E-84EB-8DFEFCFA0C382/0/2aMovingTowardsCredentialingInteroperability_7810.pdf
- "Personal Identity Verification Interoperable (PIV-I): Frequently Asked Questions (FAQ)," Version 1.0, CIO Council, June 28, 2010, http://www.idmanagement.gov/documents/PIV-I_FAQ.pdf
- "Personal Identity Verification Interoperability for Non-Federal Issuers," Version 1.1, Federal CIO Council, July 2010, http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers.pdf
- "The Realized Value of the Federal Public Key Infrastructure (FPKI)," Identity Credential and Access Management Subcommittee, Jan. 29, 2010, <http://www.idmanagement.gov/documents/RealizedValueFederalPKI.pdf>
- "Research Collaboration in the Cloud: How NCI and Research Partners Are Improving Business Processes Using Digital Identities," http://www.fips201.com/resources/audio/iab_0710/iab_072810_ansher_and_cullen.pdf
- "Spring Ahead: Federal and Mutual Aid Emergency Response Official Electronic Credentialing and Validation Interoperability Demonstration - May 19, 21, 2009," FEMA After Action Report, <http://www.dps.mo.gov/HomelandSecurity/documents/Credentialing/Spring%20Ahead%20AAR%20July%202009.pdf>
- U.S. Dept. of Justice, Drug Enforcement Administration, "Electronic Prescriptions for Controlled Substances," 21 CFR Parts 1300, 1304, 1306, 1311, Federal Register notice, Docket No. DEA-2181, RIN 1117-AA61, March 24, 2010
- "Update on GSA's ICAM Implementation to the Smartcard IAB," Bill Erwin, GSA, presentation, Smart Card Interagency Advisory Board (IAB) meeting, June 29, 2010, http://www.fips201.com/resources/audio/iab_0610/iab_062910_erwin.pdf

8 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Physical Access Council and Identity Council to describe the benefits of the FIPS 201 and PIV standards and PIV-I framework for state and local governments to enable interoperability and trust across different government issuers for a wide variety of identity credentialing programs.

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: Accenture LLP; AMAG Technology; CardLogix; CertiPath; Datawatch; Deloitte; Diebold Security; Gemalto; General Services Administration (GSA); Hewlett-Packard Enterprise Services; HID Global; Hirsch Electronics; Identification Technology Partners; IDmachines; Intellisoft, Inc.; L-1 Identity Solutions; Nagra ID; Northrop Grumman Corporation; Organization Change Future Workplace, LLC (OCFW); Probaris, Inc.; SCM Microsystems; Technica; U.S. Dept. of Defense/Defense Manpower Data Center (DMDC); U.S. Dept. of State; XTec, Inc.

Special thanks go to **Robert Donelson**, OCFW, and **LaChelle LeVan**, Probaris, who managed the project and to the following Council members who wrote content for this document:

- **Sal D'Agostino**, IDmachines
- **Robert Donelson**, OCFW
- **Lolie Kull**, Hewlett-Packard Enterprise Services
- **LaChelle LeVan**, Probaris, Inc
- **Michael Magrath**, Gemalto
- **Cathy Medich**, Smart Card Alliance
- **Steve Rogers**, Intellisoft, Inc.
- **Lars Suneborn**, Hirsch Electronics

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

- **Dave Adams**, HID Global
- **Mark Dale**, Hewlett-Packard Enterprise Services
- **Tony Damalas**, Diebold Security
- **Roland Fournier**, L-1 Identity Solutions
- **Mary Frary**, Independent
- **Bob Gilson**, DMDC
- **Walter Hamilton**, ID Technology Partners
- **Daryl Hendricks**, GSA
- **Steve Howard**, CertiPath
- **Won Jun**, ID Technology Partners
- **Harold Kocken**, Deloitte
- **Nicholas Kubiak**, DMDC
- **Gilles Lisimaque**, ID Technology Partners
- **Don Malloy**, Nagra ID
- **Bob Merkert**, SCM Microsystems
- **Neville Pattinson**, Gemalto
- **Rick Pratt**, XTec, Inc.
- **Kenny Reed**, Datawatch
- **Bruce Ross**, CardLogix
- **Dan Schleifer**, IDmachines
- **Adam Shane**, AMAG Technology
- **Brian Stein**, Accenture, LLP
- **Mike Sulak**, Dept. of State
- **Rick Uhrig**, XTec, Inc.
- **Keith Ward**, Northrop Grumman Corp.
- **Bob Wilberger**, Technica
- **Rob Zivney**, Hirsch Electronics

The Smart Card Alliance thanks the **National Association of State Chief Information Officers (NASCIO) State Digital Identity Work Group** for their comments on the preliminary version of the white paper.

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 address 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.

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

9 Appendix A: Standards Efforts

Organization	Description
<p>North American Security Products Association (NASPO)</p>	<p>NASPO is a non-profit organization that certifies that government and business organizations providing identity documents, financial instruments, and other value documents are operating under a uniform set of accepted standards and practices.</p> <p>NASPO certification is an audit process that verifies compliance with the new ANSI/NASPO Security Assurance Standard. The process begins with an assessment of vulnerability followed by the identification of any risks.</p> <p>For example, the process for an organization producing and issuing ID documents includes process certification of the entire supply chain (such as paper mill procedures to ensure a secure paper stock), printer and printing processes, and issuing procedures. All certification steps are designed to enhance trust in the final ID document.</p> <p>http://www.naspo.info/</p>
<p>National Institute of Standards and Technology (NIST)</p>	<p>The NIST Information Technology Laboratory (ITL) accelerates the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications through standards development.</p> <p>Federal Information Processing Standards (FIPS) 201 is the standard that supports both PIV credential standards for Federal agencies and PIV-I credential standards for states, local and private sector businesses.</p> <p>FIPS 201 standard: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf</p> <p>PIV-I guidance: http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf</p>
<p>American Association of Motor Vehicle Administrators (AAMVA)</p>	<p>AAMVA published the 2009 DL/ID Card Design Standard (CDS).</p> <p>The CDS provides for the design of driver licenses (DL) and identification (ID) cards. The intent is to improve the security of the DL/ID cards and the level of interoperability among cards issued by all North American jurisdictions. The standard includes machine-readable technologies as well as a test tool issuing entities can use to verify compliance with the CDS standard.</p> <p>The AAMVA Courtesy Verification Program (CVP) provides an effective way for AAMVA members to determine whether DL/ID cards using machine-readable technologies conform to the applicable AAMVA standards and specifications</p>
<p>American Bar Association Federated Identity Management Legal Task Force</p>	<p>This task force focuses on identifying and analyzing the legal issues that arise in connection with the development, implementation, and use of federated identity management systems; evaluating appropriate legal models to address issues proactively; and developing model terms and contracts that can be used by parties and more.</p> <p>The task force work is found at: www.abanet.org/dch/committee.cfm?com=CL320041</p>
<p>International Organization for Standardization (ISO)</p>	<p>The ISO JTC1 creates common criteria for international use and recognition of driver's licenses without impeding individual national and regional</p>

Organization	Description
Joint Technical Committee for Information Technology (JTC1), Subcommittee for Identification Cards and Related Devices (SC17)	<p>authorities in satisfying their own specific requirements. This standard addresses the following items:</p> <ul style="list-style-type: none"> ▪ Physical characteristics ▪ Magnetic stripe ▪ Optical memory ▪ Integrated circuit cards with contacts ▪ Integrated circuit cards without contacts ▪ Bar codes, one and two dimensional ▪ Optical character recognition ▪ Digital (digitized) images and signal <p>http://www.iso.org/iso/standards_development/technical_committees/other_bodies/iso_technical_committee.htm?commid=45020</p>
International Committee for Information Technology Standards (INCITS/M1) Biometrics Technical Committee	<p>The INCITS M1 biometrics program includes biometric standards for data interchange formats, common file formats, application interfaces, profiles, and performance testing and reporting. The goal of M1's work is to accelerate the deployment of significantly better, standards-based security solutions for homeland defense and the prevention of identity theft as well as other government and commercial applications based on biometric personal authentication.</p> <p>http://www.incits.org/</p>
XML Extensible Markup Language	<p>Published by the World Wide Web Consortium (W3C), XML comprises a set of rules for encoding documents electronically. XML's design goals emphasize simplicity, generality, and usability over the Internet. XML's design focuses on documents and is widely used for representation of arbitrary data structures (for example, in Web services).</p>
National Information Exchange Model (NIEM)	<p>NIEM is a Federal, state, local, and tribal interagency initiative that provides a foundation for seamless information exchange. NIEM is a framework created to:</p> <ul style="list-style-type: none"> ▪ Develop standards, a common lexicon, and an online repository of information exchange package documents to support information sharing ▪ Provide technical tools to support development, discovery, dissemination, and re-use of exchange documents ▪ Provide training, technical assistance, and implementation support services for enterprise-wide information exchange <p>http://www.niem.gov/</p>
National Association of State Chief Information Officers (NASCIO)	<p>NASCIO represents state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia, with the mission to foster government excellence through quality business practices, information management, and technology policy.</p> <p>NASCIO has formed the State Digital Identity Work Group to provide a consensus-based forum that enables state chief information officers (CIOs), chief information security officers (CISOs), enterprise architects, and line-of-business stakeholders to collaborate on developing recommendations on federated identity management initiatives. This working group intends to provide a framework for the key guidelines for program management and collaboration. The charter seeks to develop solutions for a sustainable and supportable model for use in identity, credentialing, and access efforts.</p> <p>http://www.nascio.org/committees/digitalID/</p>

Organization	Description
W3C	<p>The W3C mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web.</p> <p>http://www.w3.org/</p>
IETF	<p>The Internet Engineering Task Force (IETF) is an international community of volunteers. The IETF mission is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.</p> <p>IETF is open to any individual or organization interested in participating in the IETF effort to enhance operation of the Internet and related services.</p> <p>The Internet Architecture Board, (IAB) also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB.</p> <p>The Internet Assigned Numbers Authority (IANA) provides oversight and is the central coordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the Internet Society (ISOC) to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters.</p> <p>http://www.ietf.org/</p>
ICAO	<p>The International Civil Aviation Organization (ICAO) has its headquarters in Montreal, Canada, with seven regional offices throughout the world. ICAO is mandated by the United Nations to ensure the safe, efficient and orderly evolution of international civil aviation.</p> <p>To implement this vision, the Organization has established sections to address the following strategic objectives:</p> <ul style="list-style-type: none"> • Safety - enhance global civil aviation safety • Security - enhance global civil aviation security • Environmental protection - minimize the adverse effect of global civil aviation on the environment • Efficiency - enhance the efficiency of aviation operations • Continuity - maintain the continuity of aviation operations • Rule of law - strengthen law governing international civil aviation <p>Aviation safety is a key objective of ICAO and is part of the work in the following Sections:</p> <ul style="list-style-type: none"> • Aerodromes, Air Routes and Ground Aids (AGA) Section • Accident Investigation and Prevention (AIG) Section • Flight Safety (FLS) Section • Aviation Medicine (MED) Section • Flight Safety and Human Factors • Integrated Safety Management (ISM) • Flight Safety Information Exchange (FSIX) <p>http://www.icao.int/</p>