PIV-Interoperable Credential Case Studies

A Smart Card Alliance Identity Council White Paper

Publication Date: February 2012
Publication Number: IC-12001

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 4

2 BOOZ ALLEN HAMILTON PIV-I CASE STUDY 6

2.1 PROJECT TIMELINE 6
2.2 ISSUES ADDRESSED 7
2.3 REMAINING ISSUES 8
2.4 LESSONS LEARNED 8

3 SAIC PIV-I CASE STUDY 10

3.1 PROJECT OVERVIEW 10
3.2 PROJECT BACKGROUND 10
3.3 IMPLEMENTATION DESCRIPTION 10
3.4 IMPLEMENTATION TIMING 11
3.5 BENEFITS AND VALUE PROPOSITIONS 11
3.6 LESSONS LEARNED 11

4 XTEC PIV-I CASE STUDY 13

4.1 INTRODUCTION 13
4.2 PROJECT OVERVIEW 13
4.3 PROJECT BACKGROUND 13
4.4 IMPLEMENTATION DESCRIPTION 14
4.5 IMPLEMENTATION TIMING 15
4.6 BENEFITS/VALUE PROPOSITIONS 15
4.7 LESSONS LEARNED 15

5 COMMONWEALTH OF VIRGINIA PIV-I CASE STUDY 17

5.1 INTRODUCTION 17
5.2 PROJECT BACKGROUND 17
5.3 FIRST PHASE IMPLEMENTATION DESCRIPTION AND TIMING 17
5.4 FIRST PHASE LESSONS LEARNED 18
5.5 SECOND PHASE IMPLEMENTATION DESCRIPTION AND TIMING 18
5.6 NEXT STEPS 18
5.7 OTHER STATE FRAC EFFORTS 19

6 CONCLUSIONS: PIV-I BENEFITS FOR ENTERPRISES 20

7 PUBLICATION ACKNOWLEDGEMENTS 23

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 Federal Information Processing Standard, FIPS 201)[1] that create the Federal identity 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.

The Federal government has issued well over 5 million of these credentials, called Personal Identity Verification (PIV) cards, to both employees and contractors. Federal agencies use the PIV card to authorize employee access to both physical and logical resources and to assign access privileges. The success of the program is largely due to the development of goals, issuance policies, and technical specifications that all Federal agencies have agreed 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.

As the benefits of a common identity credential become clear, interest in such a credential 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 IT networks.[2] The PIV-I credential is technically interoperable with the Federal government PIV systems (e.g., readers) and is issued in a manner that allows Federal government agencies to trust the card. PIV-I credentials comply with Federal Bridge guidance on identity-proofing, registration, and issuance. PIV-I credentials are cross-certified with the Federal Public Key Infrastructure (PKI) Bridge[3] to allow contractor personnel to access authorized resources. Private enterprises can also take advantage of this technology. The Commercial Identity Verification (CIV) credential leverages the PIV-I specifications, technology, and data model without any requirement for identity proofing or PKI cross-certification.[4] Any enterprise can create, issue, and use CIV credentials to achieve whatever level of assurance is required in that enterprise's environment.

This white paper provides case studies that identify realized benefits, describe best practices, and illustrate how and why the featured organizations chose to establish an identity program using the PIV-I credential. It represents one of the first efforts to document and share information about PIV-I deployments. These case studies represent the initial enterprise deployments outside of first responder use cases. Commercial off-the-shelf physical, logical, and mobile enterprise applications are increasingly supporting PIV (and therefore PIV-I) authentication methods. This support makes it easier for enterprise IT budgets to leverage their investment in identity, credentialing, access, and security services.

As the case studies indicate, a variety of organizations, including large corporations, consulting firms, and state and local governments, are all beginning to deploy PIV-I solutions. While each entity has its own specific reasons for doing so, certain common drivers are beginning to emerge:

- *Economies of scale*. As PIV and PIV-I credentials gain marketplace traction, the card and card reader become commodities and supporting middleware is available in popular

[1] National Institute of Standards, Draft FIPS PUB 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* March 2011, http://csrc.nist.gov/publications/PubsFIPS.html.

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

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

[4] Smart Card Alliance, *Commercial Identity Verification(CIV) Credential–Leveraging FIPS 201 and the PIV Specifications*, October 2011, http://www.smartcardalliance.org/pages/publications-the-commercial-identity-verification-civ-credential-leveraging-fips-201-and-the-piv-specifications.

operating systems, helping reduce the cost of implementation, speed deployment and simplify use.

- *Published credential standard*. The credential is based on the open, published NIST PIV and related standards, making it easier for software providers and developers to enable an increasing number of applications to use the credential.
- *Interoperability*. As the PIV-I credentials are based on NIST and other standards, developers can leverage this to allow its use across a variety of applications and devices. For example, individuals can use one credential to access offices, the parking garage, and client locations and networks (if a trust relationship is established).
- *Fewer credentials*. The ultimate goal is to reduce the number of identity credentials that individuals must carry and/or remember in order to prove that they are who they claim to be.
- *Identity assurance*. Individuals with PIV-I credentials have been verified through an identity proofing process and enrollment system, and entities can rely on a base level of identity confirmation,
- *Privacy and secure web and messaging applications*. Use of the PIV-I credential allows for the secure transfer and storage of data and messages using encryption and digital signatures.
- *Remote access*. PIV-I credentials use smart card technology and can offer strong authentication for remote and wireless access to corporate networks.

2 Booz Allen Hamilton PIV-I Case Study

In 2008, Booz Allen launched Operation Sentinel, a comprehensive multi-year program to transform their information security posture. One of the key initiatives of Operation Sentinel was to improve network security by migrating to PKI-based authentication. Because this initiative coincided with the development of the PIV-I specification, Booz Allen tied the process and technology requirements to the emerging PIV-I requirements.

An initial step in Operation Sentinel was to create a broad-based governance structure to review requirements, design and implement solutions, and provide training and oversight to ensure that solutions are consistently followed and effective. Participation by representatives from across a wide range of internal and client facing teams in the Operation Sentinel governance structure allowed Booz Allen to begin to issue the new smart card-based identity cards to all Booz Allen staff.

2.1 Project Timeline

Figure 1 illustrates key milestones of Operation Sentinel. The left side of the figure shows the maturation of the PIV-I requirements, starting with the publication of *Personal Identity Verification Interoperability For Non-Federal Issuers*[5] in May 2009 and ending with the finalization of the requirement, and a process for certifying commercial issuers against those requirements, in May 2010.[6] The right side shows key milestones in the implementation of Booz Allen's new identity cards.

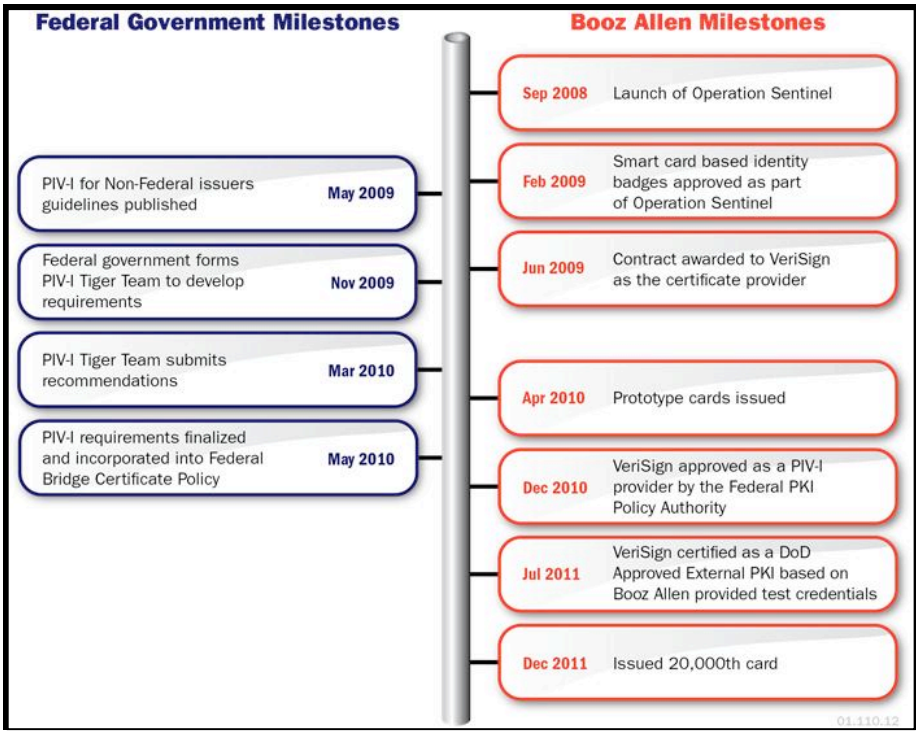


Figure 1. Key Milestones for Operation Sentinel

[5] Federal CIO Council, *op. cit*.

[6] Certification is described in Federal Bridge Certification Authority, *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) version 2.25*, December 9, 2011, http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf.

2.2 Issues Addressed

Successful development and deployment of new corporate identity cards meeting the PIV-I standard required Booz Allen to resolve several issues:

- Privacy issues connected with biometric data capture
- Card layout requirements
- System integration

2.2.1 Biometric Data Capture

The PIV-I specification requires the capture and storage of biometric data (two fingerprints and a facial image). However, because of privacy considerations, Booz Allen does not require the capture of biometric data as a condition of employment. To address this issue, Booz Allen implemented a non-PIV-I smart card that can be issued to individuals who decline to submit their fingerprints. These cards are fully functional within Booz Allen but are not enabled for Federal Government interoperability.

2.2.2 Card Layout

There were competing and overlapping requirements for the information that had to be displayed on the front of the card; Booz Allen spent considerable time trying to resolve these many requirements. The PIV-I standard stated what information (e.g., photo, name, card expiration date, company name and affiliation) must be printed on the card. In addition, the Department of Defense (DoD) Defense Security Service required Booz Allen's physical security team to add other specific card elements (e.g., if they were a contractor, which firm they were associated with, plus additional printed security features).

By working with Booz Allen's internal security, marketing, compliance, and legal teams, all required information was able to be placed on a card that measures 2-1/8in by 3-3/18in. Additional security features, including microprinting, were added to the card by working closely with the card vendor. The final card met the PIV-I requirements as well as all other requirements.

2.2.3 Integration with Current Systems

The new card management and card printing systems needed to be integrated with the third-party certificate provider and with internal databases such as PeopleSoft® (Oracle International Corporation) for human resource services and Active Directory® (Microsoft Corporation) for logical access. Information services staff, paired with experts from the client-facing staff, were able to complete the design and integration for both the initial pilot and for the phased rollout.

Booz Allen facilities have a physical access system which includes badge readers on external doors and hallway doors in large office buildings. Because of the expense that would be incurred to replace these readers, it was imperative that the new identity cards operate seamlessly with the existing system. The design team worked closely with the card stock vendor to ensure that the contactless interface used by the physical access system was supported by the cards. The issuance process included integration with the backend physical access control system to provide necessary data for access control.

The prototype implementation tested the use of PIV-I identity cards to log on to the Booz Allen Microsoft-based network, and to sign and encrypt email. As rollout of these credentials is completed, other Booz Allen internal systems will be enabled to support or require certificate-based authentication.

2.3 Remaining Issues

The following critical issues remain to be addressed:

- Transition to the latest algorithms
- Acceptance by Federal agencies
- Consideration of international privacy requirements

2.3.1 Algorithm Transition

Because of technical interoperability considerations, both with Booz Allen internal systems and with their Federal agency partners, the certificates on the Booz Allen identity cards are digitally signed using the SHA-1 hash algorithm. The Federal Bridge Certificate Policy requires that signatures on certificates generated after December 31, 2010 use the SHA-256 hash algorithm. Booz Allen continues to work with vendors to resolve compatibility issues and implement required changes to fully support SHA-256 on desktops and corporate information systems. Booz Allen will make a final decision regarding the transition date for SHA-256 based on this migration and the interoperability needs of Federal agency partners.

2.3.2 Federal Agency Acceptance

Booz Allen's decision to migrate to a smart card-based identity card was an internal decision based on many factors, primarily the desire to improve their internal information security. Booz Allen committed to meeting the PIV-I requirements, even when those requirements increased the overall cost of deployment, to meet identified government best practices. Booz Allen is hopeful that Federal agency partners will accept credentials that meet the PIV-I standard and will be able to benefit from the effort that Booz Allen and others across the industry have made in providing secure, interoperable credentials to their staff.

2.3.3 International

PIV-I is a United States (U.S.) standard, which creates issues for organizations with an international reach such as Booz Allen.

PIV-I identity proofing requires the presentation of credentials that are listed on the *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*.[7] Because the original intent for this form is to confirm eligibility for employment in the U.S., non-U.S. persons cannot meet these requirements. As a result, Booz Allen must currently issue non-PIV-I smart cards to these employees.

As Booz Allen works to issue new smart cards to their non-U.S. based employees, the different privacy laws of those countries must be addressed, including significant restrictions on what data can be collected, how and where it can be stored, and whether it can be exported to a U.S.-based corporate data store. The implementation team continues to work with the Booz Allen legal department to identify privacy and data protection requirements that allow for an implementable solution.

2.4 Lessons Learned

Early in the process, Booz Allen recognized that smart card technology was relatively new and operational experience was limited. Booz Allen leveraged staff with experience supporting Federal agency deployments of PIV cards and DoD Common Access Cards (CAC) to help guide the deployment. Although deployment began prior to the release of the final PIV-I specification,

[7] U.S. Immigrations and Customs Enforcement (ICE), USCIS, http://www.uscis.gov/I9

Booz Allen's experience with PIV resulted in only minor changes being required to meet final requirements.

Booz Allen's experience indicates that the following items are critical to the success of a long-term PIV-I solution:

- A clear plan outlining the design, the deployment, application enablement plans, and communications to employees is critical. The plan provides the detail that everyone can work from.
- Communications are critical; communications need to be regular, consistent and timely. Booz Allen's internal Project Management Methodology (PMM) has assisted in developing and implementing a consistent, structured communications plan.
- Plan for the transition of existing legacy credentials. Because PIV-I credentials can provide both physical and logical access, it is important to consider the impact of a user standing outside in the freezing rain who can't enter a facility or office, in addition to issues with inability to logon to workstations or Booz Allen systems.
- Implement a solution that allows for full life-cycle management of the credential including personal identification number (PIN) management, certificate updates, revocation, and key recovery. A key focus was minimizing the need for a user to visit a specific office to accomplish a task. The solution requires functionality be pushed to the desktop, enabling end user self-service.
- Multiple concurrent credentials (e.g., PIV, PIV-I, and CAC) need to be supported. Users may require two smart card readers for their machines; one for the smart card that will allow them to logon to their computer, and the second to gain access with a second card to a government website that does not yet support PIV-I. Based upon policy settings, the removal of the first card may cause the machine to immediately lock, thus not allowing use of the second card. The ability for the user to manage their multiple credentials is critical.
- Mobile devices are not yet at the point to support PIV-I credentials. The overall corporate authentication solution needs to support the management of multiple credentials for one user, such as a PIV-I card for workstation access, a secure microSD card for the mobile device, and a smart card technology-based USB device that allows credentials to be easily used within a data center (i.e., plug in the USB device and the system sees it as a smart card).
- Supporting a large variety of email clients is a requirement; it is no longer sufficient to only address the corporate mail solution. In addition to Outlook® (Microsoft Corporation) clients, Booz Allen is now looking to support Apple devices (based on IOS™ [Apple Inc.] and Mac OS X® [Apple Inc.] platforms), BlackBerry® (Research in Motion Limited) smart phones, Android™ (Google)-based phones, and Windows® (Microsoft Corporation) mobile devices.
- Certificate trust at the enterprise level presents unique challenges as to what should be trusted. Two-way, cross-organizational trust, such as the Federal Bridge, creates additional concerns that must be addressed.

Booz Allen Hamilton has extensive experience in using smart card technology for business. They have provided support to the DoD CAC implementation for over seven years and used this experience in their deployment of PIV-I. Booz Allen believes that by being an early adopter of the PIV-I standard, they will be able to take advantage of the functionality, flexibility, robustness and interoperability that it offers in maintaining a secure environment. Booz Allen plans to continue to work with their clients and partners in implementing their PIV-I solutions to allow for enhanced security in their collaboration activities.

3 SAIC PIV-I Case Study

As a major systems integrator, SAIC works within a complex ecosystem of customers, teammates, subcontractors, and vendors. Trust is of paramount importance, especially when handling sensitive information that is proprietary, personally identifiable, or export controlled. In 2012, SAIC will begin deploying PIV-I credentials to employees who need them for facilities access, strong authentication, or digital signatures or encryption.

3.1 Project Overview

SAIC has been using smart cards since 2004 and issuing smart card badges to its U.S. employees since 2007. SAIC currently issues all employees a badge that combines facilities access, computer access, and digital signature and encryption in a single form factor. The SAIC smart card badge was one of the most technologically advanced employee badges in the world when it was first deployed.

To adopt PIV-I, SAIC requires a solution that can support approximately 41,000 employees at hundreds of locations worldwide. A major challenge for SAIC is to migrate to the open standards PIV technologies, while building on the success of the previous smart card program. The solution must support physical and logical access without major changes or modifications to the facilities and computer systems that already support the legacy badges.

3.2 Project Background

A PIV-I deployment involves a number of components, including PKI, a smart card management system, and multiple card technologies. One key decision for SAIC will be to determine which components to deploy and manage internally as opposed to externally with either a software-as-a-service provider or a cloud-based solution.

A second major factor is business functionality. SAIC has a robust and cost-effective strong authentication program, and it is important that the PIV-I solution provide equivalent or greater capabilities, including the following:

- Combined physical and logical access control with support for multiple systems, including magnetic stripe, proximity, and contactless, built into a single card
- Robust emergency access for situations where a user has no identity credential token but still needs access to enterprise systems
- Digitally signed and encrypted email service using low-assurance software certificates on BlackBerry® (Research in Motion Limited) devices and other non-Windows devices
- Alternate form factors for smart card credentials, including fobs that can plug into a computer's USB port without needing a smart card reader
- Multiple copies of user credentials that can be used on different systems simultaneously

3.3 Implementation Description

SAIC has been using smart card technology since 2004; this use has improved security, streamlined operations, and increased accountability. Most important, SAIC has found that deploying PKI and smart cards enterprise-wide has resulted in benefits that add up to more than the sum of their parts.

SAIC currently uses or is considering smart card technology for the following purposes:

- Strong authentication for remote and wireless access to corporate networks
- Encryption of email messages containing sensitive and regulated information
- Digital signatures for "official" corporate email correspondence

- Digital signatures to make internal forms and processes “paperless”

3.4 Implementation Timing

SAIC is planning to deploy its PIV-I infrastructure capability in 2012, with enterprise rollout to be completed over a multi-year period.

3.5 Benefits and Value Propositions

SAIC’s greatest business case challenge for the adoption of PIV-I is that SAIC has already deployed a robust smart card and strong authentication solution. Some key considerations include the following:

- Ensure that PIV-I does not cost significantly more than the smart card strong authentication systems currently in use.
- Ensure that PIV-I does not require replacing existing smart card and badge infrastructures.
- Enable seamless interoperability between SAIC and its vendors, teammates, and customers, including using SAIC cards on teammate’s and customer’s computers (and vice versa).
- Take advantage of widespread and rapidly growing support for PIV on Windows, Mac® (Apple Inc.), Linux® (Linus Torvalds), and mobile devices.
- Take advantage of the PIV standards to drive down the costs of procurement, integration, deployment, and operation of an enterprise smart card solution.

3.6 Lessons Learned

Smart card technology is still relatively new, and SAIC found that operational experience is limited to niche uses, specific applications, and restricted communities. However, this situation is changing in the U.S., thanks to the PIV standard and the leadership of the Federal Government. Over the past seven years, organizational and technological support for smart cards has increased dramatically.

At the same time, numerous hurdles must be overcome before smart card authentication can be regarded as mainstream at the enterprise level. In addition, better integration is needed of multiple strong authentication mechanisms to support effective and secure alternatives when a smart card has been lost or stolen or if there is no reader.

Specifically, SAIC has identified the following considerations:

- Managing certificate trust at an enterprise level can be very challenging, especially when cross-organizational trust is involved, such as through the Federal Bridge.
- Authentication systems have difficulty providing for alternative authentication in the case of a lost card. This situation can create computer logon problems.
- Smart card authentication is very powerful when it is combined with an alternative, strong authentication technology, such as a one-time password. Having both forms available makes it possible to handle more use cases gracefully.
- Deploying signed and encrypted email systems enterprise-wide requires support for non-Windows users, mobile users, and Web access users.
- Users who use a smart card to logon to their computer, and then need to use a different smart card to access a Web site from that computer, will need two smart card readers in order to be able to simultaneously use both smart cards. This is problematic, as most computers are only equipped with a single reader, and removing the smart card used for computer logon causes that computer screen to lock, preventing use of the other card.

- In a data center that uses smart card authentication, USB fobs incorporating smart card technology are much more useful since this would eliminate the need to have smart card readers on all servers.
- Using digital signatures for document signing and workflow is extremely useful but requires buy-in from the process owners and users, who may be skeptical of the change. In addition, implementations vary widely and are not always intuitive.

SAIC has amassed a great deal of experience in effectively and cost-effectively using smart card technology for business purposes. SAIC is firmly committed to smart card technology as an integral part of its enterprise security program and looks forward to migrating that platform to PIV-I in the coming year. By adopting PIV-I, SAIC hopes to take advantage of the functionality, flexibility, robustness, and interoperability of this emerging standard while maintaining the current foundation of strong security.

4 XTec PIV-I Case Study

XTec Incorporated, a provider of security and authentication systems, is one of the earliest enterprises certified as a PIV-I provider. Certification prompted XTec to adopt PIV-I as its own corporate identity credential.

4.1 Introduction

As a PIV credential and solutions provider to the Federal Government, XTec adopted the PIV-I credential to be interoperable with both Federal and PIV-I customers. Adopting the secure credential also allowed XTec to use XTec product offerings for identity management and physical and logical access control.

4.2 Project Overview

XTec phased out legacy identity cards, creating an enterprise access control environment that supported CAC, PIV, PIV-I, and CIV credentials and the associated identifiers (i.e., Federal Agency Smart Credential Number (FASC-N), Global Unique Identifier (GUID)). Both physical and logical access control resources operate on a common platform.[8] This interoperability allows XTec employees to use their Federally issued CAC and PIV cards to access XTec facilities, while the PIV-I credential secures company logical and physical resources.

XTec implemented an end-to-end solution that provides PIV-I credentials, identity management, and logical and physical access control throughout the enterprise. The system is accompanied by peripheral enrollment and issuance stations, which are used to enroll employees and perform identity verification to Level 4 as specified in the NIST *Electronic Authentication Guideline*[9] and the Federal CIO Council's *Personal Identity Verification Interoperability For Non-Federal Issuers.*[10]

4.3 Project Background

The main goals for the XTec PIV-I deployment include the following:

- Secure the corporate infrastructure.
- Enable all resources to use smart cards and move everyone to a single platform.
- Implement XTec products and solutions internally.
- Gain acceptance of PIV-I by external relying parties.

XTec initially decided that PIV-I credentials would only be issued to personnel with a government security clearance. This decision reflected the possibility that future acceptance of PIV-I credentials by an external entity, such as a Federal agency, would be more likely if those credentials belong to cleared personnel. However, a background investigation is not required to obtain a PIV-I credential; some XTec PIV-I customers choose not to require such an investigation.

XTec already used a secure smart card credential for physical access control and was able to phase out the legacy credential while maintaining secure facility access. XTec locations were

[8] Outlined in National Institute of Standards and Technology, Special Publication 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.

[9] National Institute of Standards and Technology, Special Publication 800-63-1, *Electronic Authentication Guideline,* December 2011, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf.

[10] Federal CIO Council, *op. cit*.

equipped with infrastructure components such as domain controllers, card readers, and internal network applications. XTec expanded this infrastructure by implementing a centralized access control monitoring solution. This solution allows administrators to monitor physical and logical access requests at all corporate locations from one central Web application. All cardholders also had the option of using self-service card maintenance products to unlock credentials and change their PIV-I PIN.

4.4 Implementation Description

XTec used its own identity management and physical and logical access control products and services to achieve PIV-I deployment and to implement the use of the PIV-I credential for everyday access control. XTec fully implemented physical access control during the first phase of PIV-I credential issuance; the initial infrastructure supported legacy access control IDs as well as newly issued PIV-I credentials, PIV, and CAC cards. Cardholders were able to take advantage of electronic entry and verification, both internally and at the perimeter. Deployment allowed for full use of the card capabilities, including PIN entry, biometric verification, and challenge-response protocol.

The first phase of logical access control, which began with initial PIV-I issuance, is currently operating in one division. Cardholders are able to log onto their computers with the PIV-I credential and then authenticate for various applications. XTec is currently testing enterprise logical access control at all corporate locations and expects to have full logical access control in production during the first quarter of 2012.

Table 1 lists the capabilities of the current implementation and indicates how XTec plans to enhance them.

Table 1. Current and Future Capabilities of the XTec PIV-I Implementation

Current Capability	Future Capability
Self-service PIV-I maintenance (desktop and kiosk)	Key recovery
PIN change, card unlock	Email encryption
Biometric authentication	Digital signature
Printed security features	Visitor management
Emergency contact information	Single sign-on (including mobile)
Employee specific messages and alerts	Mobile monitoring
Web-based management and administration	—
Identity and card cryptographic authentication	—
Online Certificate Status Protocol (OSCP) responder services	—
Certificate updates	—

4.5 Implementation Timing

PIV-I credentials were initially issued to employees with an active Top Secret clearance. Shortly thereafter, the company issued PIV-I credentials to employees with an active Secret clearance. Employees who do not require logical access will be issued a CIV credential, which is technically interoperable with the PIV-I credential but cannot be trusted by Federal relying parties. This hybrid approach allowed XTec to move all employees to one interoperable, secure platform while simultaneously meeting specific business needs.

XTec utilizes full cryptographic authentication at all entry points and equipped corporate locations with a variety of HSPD-12 compliant card readers, including contact, contactless, PIN and biometric physical access control readers. All readers can be monitored, audited, configured, and updated from one Web-based interface that is accessible only to administrators with the proper permissions.

The final phase of PIV-I deployment will occur during the last quarter of 2011 and the first quarter of 2012. This phase will include issuing PIV-I and CIV credentials to all remaining XTec employees and fully incorporating logical access control. During the first quarter of 2012, XTec will implement email encryption, digital signatures, and mobile capabilities for everyday communication. The final objective for PIV-I implementation is for the credentials to be accepted by an external entity, such as a Federal, state, or local government entity or a financial institution.

XTec paid particular attention to credential lifecycle management throughout the deployment process. To reap the benefits of investing in a PIV-I enterprise solution, XTec anticipates that the credentials issued will have to support future enhancements and changes. Preparing for lifecycle processes such as PIN management, certificate updates, and key recovery are essential to a successful, sustainable PIV-I infrastructure.

4.6 Benefits/Value Propositions

Overall, XTec employees and management were encouraged by the added security offered by PIV-I credentials. Employees appreciated the convenience of fast authentication; managers were comforted by the assurance of strong cryptographic authentication. Logical access control provides obvious benefits to everyone and enhances the security of the network and company information. It helped establish trust throughout the organization and allowed XTec to streamline its internal processes. XTec can now demonstrate interoperability to customers while securing its own infrastructure and resources.

4.7 Lessons Learned

As a provider of solutions for PIV-I credentials, identity management, and physical and logical access control, XTec was able to deploy PIV-I quickly to secure its facilities and information resources. Lessons learned from numerous HSPD-12 deployments gave XTec insight into planning for future PIV-I technical and policy enhancements.

XTec focused on maintaining and updating the PIV-I credentials and infrastructure easily. Cardholder self-management was deployed to maintain the PIV-I credential on a daily basis, while programmable card readers and Web-based configuration maintain the infrastructure. The PIV-I credential is an interoperable, secure credential that serves as a centerpiece for the identity ecosystem of the XTec corporate enterprise.

XTec's experience indicates that the following factors are crucial to implementation of a successful long-term solution:

- The ability to support legacy credentials while transitioning to PIV-I credentials, leaving no gap in secure physical facility access.

- The capability to support the full lifecycle of the credential: PIN management, certificate updates, revocation, and key recovery are all essential to return on investment of the program.
- The ability to extend functionality to the desktop. Significant cost savings are projected by empowering credential holders to manage their own credentials after completing strong authentication.
- The ability to change authentication mechanisms for physical access control. This ability accommodates XTec visitors whose PIV or CAC credentials use asymmetric authentication. Meanwhile, XTec employees with PIV-I credentials can easily authenticate their credentials through symmetric authentication.

5 Commonwealth of Virginia PIV-I Case Study

The events of September 11, 2001 made it imperative for the National Capital Region (NCR) to have a method for rapidly authenticating and validating emergency responders. While the majority of emergency responders already had identification cards, their credentials were not recognized at all levels of government or by different jurisdictions. The incident commanders on site either had to assume that people were who they said they were, or they had to deny or delay access of critical emergency personnel to the crash scene at the Pentagon.

5.1 Introduction

In a desire to improve security in the NCR, the Commonwealth of Virginia Governor's Office of Commonwealth Preparedness (OCP), now known as the Office of Veterans Affairs and Homeland Security (OVAHS), decided in 2005 to appropriate a portion of a grant awarded by the NCR Urban Areas Security Initiative to use FIPS 201 technology to deploy a credential that is interoperable at all levels using the standard. The intent was to enhance not only Virginia's response and recovery efforts but those of the nation as well, so that credentialing no longer delays those efforts in any scenario requiring the deployment of emergency responders.[11]

The result was a pilot implementation of the First Responder Authentication Credential (FRAC) program.

5.2 Project Background

The Commonwealth of Virginia's FRAC program was the first pilot program of its kind nationwide.

The main goals for the credential, which in its latest version is a smart card meeting the PIV-I standard, include:

1. Rapidly authenticate (electronically) the identity of a person at the scene of an incident.
2. Electronically authenticate a first responder's key skills so that incident commanders can assign personnel to tasks quickly and appropriately.
3. Provide a level of trust between emergency responders across multiple jurisdictions in times of critical incidents, thus enhancing cooperation and the efficiency of the response efforts between Federal, state, regional, local, and private sector emergency personnel.[12]

5.3 First Phase Implementation Description and Timing

The first phase of Virginia's FRAC program focused on providing credentials to those jurisdictions responsible for responding to Federal facilities (including the Pentagon) in case of emergency. Implementation began in 2005 and continued into 2006. During a four-month period, with the help of a number of different vendors, the Commonwealth issued over 2,200 FRACs in Arlington County and the City of Alexandria.

The credentials issued during this phase expired by March 2010, when the pilot program concluded. Since the Commonwealth's initial FRAC program was a pilot program only and since physical access control systems (PACS) and logical access control systems (LACS) were not widely available to use with the FIPS 201 technology, FRAC holders had retained their legacy access cards and systems and were able to continue using them.

[11] Commonwealth of Virginia First Responder Authentication Credential (FRAC) Program Update, W. Duane Stafford, Statewide Credentialing Coordinator Secure Commonwealth Panel, October 2010.
[12] Ibid.

5.4 First Phase Lessons Learned

The first phase of the Virginia FRAC pilot project taught a number of lessons. First, the FIPS 201 standards were still being developed at project rollout, necessitating a few changes to the pilot program. In particular, the technical and policy requirements for cross-certification to the Federal Bridge Certificate Authority for the PIV-I credential did not exist. Furthermore, the FRAC was not fully integrated with existing PACS or LACS, so it was not widely used on a daily basis. Over time, the FRAC was used for some physical access control using a mobile smart card reader; however, use for logical access control was not available. Since that time, commercial off-the-shelf products, including PACS, operating systems (e.g., Windows, MacOS® [Apple Inc.]) and applications (e.g., Outlook , Mozilla® [Mozilla Foundation]) have provided support for logical and physical access use cases.

Because this program was the first of its kind, certain guidelines for the PIV-I FRAC had not yet been established. Thus, the topographical design was similar, though not identical, to the design that previously had been established for the Federal PIV cards.[13]

Other lessons learned during the first phase included the need for the FRAC to be used in a cardholder's day-to-day activities so that the card would be accessible in an emergency situation. Additionally, since mobile card readers were not widely deployed outside of the Pentagon, the cards were not utilized at their full potential. Finally, because of the grant lifecycle, Virginia only had a few months to issue over 2,200 FRACs to Arlington County and Alexandria. The only way to accomplish this was through the use of contractors. After issuance was completed, all of the equipment used to issue the FRACs was returned to the contractor, limiting the ability for Arlington and Alexandria to invest local resources in the program.

These lessons helped identify the changes needed for the second phase of the program.

5.5 Second Phase Implementation Description and Timing

The second phase of the Commonwealth of Virginia's FRAC program is taking place in the Hampton Roads region of Virginia. This phase began in late 2008, when additional Department of Homeland Security grant funding was secured and a Hampton Roads Regional Credential Working Group was formed. This phase includes both public and private participation[14] and the goal of determining standard operating procedures (SOP) for the specific locations using the cards, in addition to using them for incident scenes.

The second phase of the FRAC credentialing effort utilizes a managed service offering (MSO) which includes hardware, software, support, and services for the issuance of 13,000 PIV-I FRACs. Eight enrollment and issuance stations have been deployed and designated firefighters, police officers, administrators and emergency management personnel have been trained on how to issue these credentials within their jurisdiction. Thirty-nine mobile handheld smart card readers have been purchased and are being deployed for mobile identity and attribute validation using the handhelds.

5.6 Next Steps

The next step for the Commonwealth of Virginia is to expand the FRAC/PIV-I program within Northern Virginia using additional available grant funding. The plan is then to expand into Central

[13] First Responder Identity Credentials, Mike McAllister, Critical Infrastructure Protection Coordinator, The Governor's Office of Commonwealth Preparedness, Smart Cards in Government Conference, October 2008

[14] Commonwealth of Virginia First Responder Authentication Credential (FRAC) Program, Smart Cards in Government Conference, Mike McAllister, Critical Infrastructure Protection Coordinator, The Governor's Office of Commonwealth Preparedness, Smart Cards in Government Conference, October 2009

Virginia and the remainder of Virginia. Furthermore, FRAC/PIV-I cards are to be issued not only to emergency responders, but also to critical infrastructure key responders, such as the people responsible for Virginia's water supply and power grid.

The Commonwealth of Virginia's FRAC program is a certified PIV-I program. As a result, the Commonwealth has taken a number of additional actions that support the use of a PIV-I credential. For example, on March 26, 2011, during the 2011 Session of the Virginia Acts of Assembly, the Commonwealth approved use of the PIV-I credential in electronic notary acts.[15] In January 2011, the Virginia House introduced a bill[16] that reduces the liability of providers and users of digital identity credentials that are cross-certified to the Federal Bridge, making this the first legislation to tie economic benefits to PIV-I credentials. These two examples illustrate how the PIV-I has evolved in the Commonwealth of Virginia and demonstrate the Commonwealth's desire to increase the return on investment of the PIV-I credential.

5.7 Other State FRAC Efforts

The Department of Homeland Security and the Federal Emergency Management Agency (FEMA) have been working with many states on deploying FRACs, 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.[17]

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.[18]

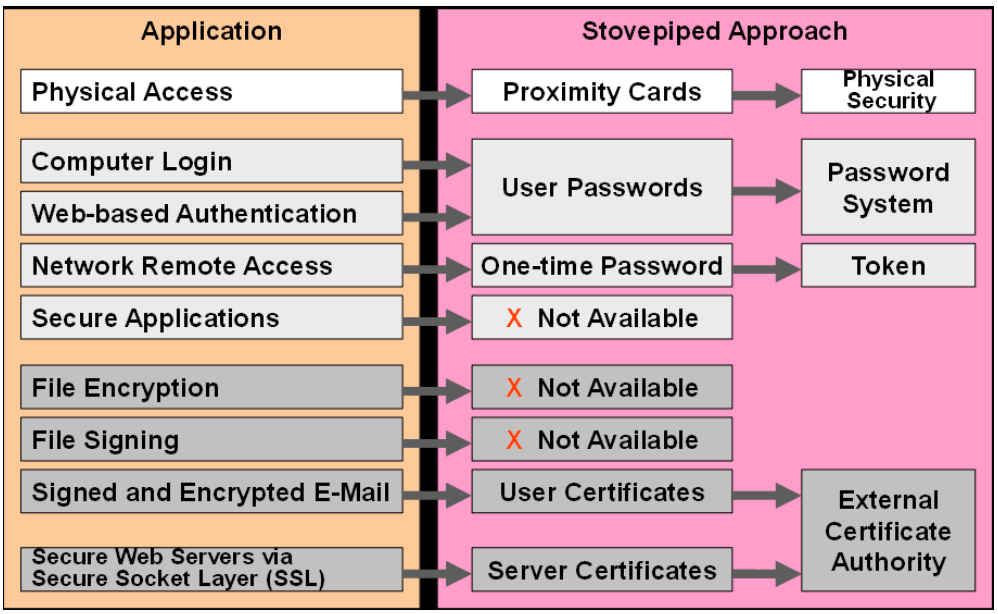
[15] SecureIDNews, "Virginia law enables electronic notarization," April 13, 2011, http://www.secureidnews.com/2011/04/13/virginia-law-enables-electronic-notarization.
[16] House Bill No. 2259, 2011 Session, http://lis.virginia.gov/cgi-bin/legp604.exe?111+ful+HB2259.
[17] "Moving towards Credentialing Interoperability: Case Studies at the State, Local and Regional Level," U.S. Department of Homeland Security, July 2010[17]
[18] PIV-I/FRAC Technology Transition Working Group, U.S. Department of Homeland Security Command, Control and Interoperability Division

6 Conclusions: PIV-I Benefits for Enterprises

As the case studies illustrate, PIV-I is a technology that is continuing to mature. Each organization discussed in this white paper is involved at a different stage of deployment and adoption. SAIC has entered the planning phase of their PIV-I deployment, the Commonwealth of Virginia has completed their pilot, XTec has successfully completed the initial deployment phase, and Booz Allen Hamilton is completing deployment.

Figures 2 and 3 illustrate the benefits of a PIV-I based solution.

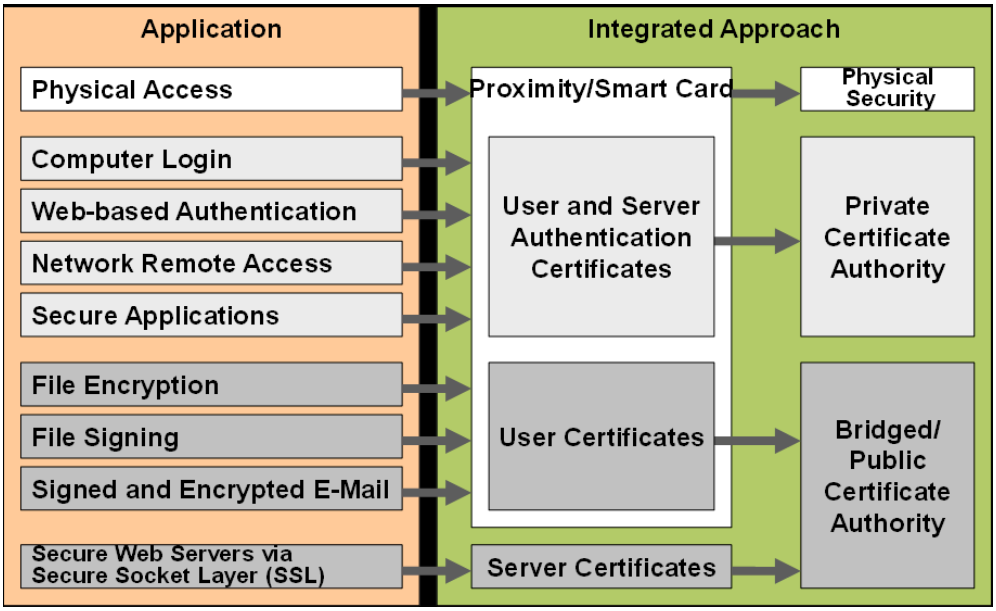
Figure 2: Current Enterprise Implementations



Many organizations today have legacy "stovepipe" solutions for their physical access, computer login, Web-based authenication, network remote access, secure applications, file signing/encryption, signed and encrypted email, and secure Web servers that use Secure Sockets Layer/Transport Layer Security (SSL/TLS). Each application area requires a unique solution. Physical access uses a proximity card that is managed by a physical access control system. Computer login is usually managed by a centralized user management system. Network remote access uses a one-time password that is then managed by yet another system that is responsible for the tokens that are deployed. Secure email requires user certificates that are issued by an external certificate authority for interoperability with other organizations. SSL certificates are issued by an external certificate authority so that others can trust the site they are acessing.

A PIV-I based solution helps to remove the number of "stove pipes" that require management. It can also help in reducing the number of support issues since there are fewer credentials to be remembered.

Figure 3: Enterprise PIV-I Implementations



In the PIV-I solution, one card provides physical access via the contactless interface whether the system is reading a certificate on the card or reading a legacy identifier via a proximity antenna. Computer login, Web-based authentication, network remote access, and secure applications can take advantage of the user certificates that are stored on the card; these can be issued from either a public or private certificate authority. For file encryption, file signing, and signed and encrypted email, user certificates issued from a bridged/public certificate authority are normally used. Secure Web servers using SSL or TLS use server certificates that are normally issued from a public certificate authority. The choice among bridged, public and private certificate authorities is dictated by the organization's policy and plans for interoperability; each has its own unique set of requirements.

The lessons learned by these organizations are many. While each provided highlights that they feel are noteworthy, the following are common threads among them:

- Implementing a smooth transition to the new PIV-I credential is critical for success.
- Full life-cycle support for the credential is needed, with as much as possible being performed by the users.
- The implementation needs to support multiple types of authentication credentials (PIV-I, PIV, CAC) and form factors (card, secure microSD, USB smart cards) for a single user.
- Deploying signed and encrypted email systems enterprise-wide requires support for non-Windows users, mobile users, and web access users.
- Managing certificate trust at the enterprise level can be a challenge, especially when two-way trusts are involved, such as cross-certification with the Federal Bridge.

All organizations concluded that PIV-I offers significant benefits.

- There are economies of scale from expanding use of the PIV credential as readers and software become commoditized.
- As individuals become accustomed to using smart-cards, their speed to access secured networks or applications will increase.

- The fact that the technology is based on open standards provides interoperability, both among vendor products and among different organizations using the standards.
- Multiple suppliers offer products and services that support PIV-I credentials, reducing costs and providing a choice of vendors.
- The implementation of the PIV-I identity proofing process and strong authentication technologies improves security for an organization's physical facilities and information systems.
- All Federal agencies have now implemented PIV credentials, allowing organizations to build their infrastructure using proven technology that has industry-wide acceptance.
- PIV-I cards support multiple applications, allowing an individual to have one card that can be used for physical access and for different logical access applications. A single credential per individual represents a significant cost savings in the long term.
- Using PIV-I credentials for logon can simplify the logon process while increasing security and improving user convenience and ease of use.
- By building on open standards and a technology platform with an open architecture, organizations can future-proof their systems and add capabilities after initial implementation.
- PIV implementations have proven to be scalable to millions of employees, supporting the largest organization's requirements.

Today, the Federal government continues to encourage state and local governments to adopt PIV-I.[19] The aerospace industry and many large Department of Defense contracting firms have begun deploying PIV-I credentials due to the requirement to interface with the Federal Bridge. Current pilot projects are testing a requirement that companies providing the military with services (such as vending machines, copier services, food delivery, and other contracted services) provide credentials that are PIV-I-compliant for their staff members to gain access to the military installations where the company holds a contract.

A successful implementation requires the convergence of two operational teams: a logical access control team and a physical access control team. For most organizations considering whether to adopt this technology, cross-organizational involvement in the implementation will be a change in view. This change in viewpoint requires both short- and long-term planning. Deploying the new cards may be easy; determining how and where they are used takes time and significant testing.

[19] Department of Homeland Security, "NIMS Guideline for the Credentialing of Personnel," July 2011, http://www.fema.gov/pdf/emergency/nims/nims_alert_cred_guideline.pdf.

7 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Identity Council to document the benefits of using PIV-interoperable credentials for enterprises and to provide implementation case studies of enterprises that are issuing or planning to issue PIV-I credentials.

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

The Smart Card Alliance wishes to thank the Identity Council members for their contributions. Participants involved in the development of this white paper included: Booz Allen Hamilton; Consult Hyperion; Datacard Group; Deloitte; Diebold; GSA; HP Enterprise Services; IDenticard; Identification Technology Partners; Identive Group; IDmachines; Intellisoft, Inc.; NagraID Security; NXP Semiconductors; Probaris; SAIC; Tyco Software House; Xtec, Incorporated.

Special thanks go to **Frazier Evans**, Booz Allen Hamilton, who managed the project. The Smart Card Alliance thanks the following Council members who developed case studies for this document:

- **Mari Devitte**, XTec, Incorporated
- **Frazier Evans**, Booz Allen Hamilton
- **Diana Loughner**, IDenticard
- **Chris Williams**, SAIC

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

- **Mike Berman**, Datacard Group
- **Sal D'Agostino**, IDmachines
- **Tony Damalas**, Diebold
- **Mari Devitte**, XTec, Incorporated
- **Frazier Evans**, Booz Allen Hamilton
- **Margaret Ford**, Consult Hyperion
- **Walter Hamilton**, ID Technology Partners
- **Daryl Hendricks**, GSA
- **Dan Hudson**, Datacard Group
- **Brent Iles**, Datacard Group
- **Harold Kocken**, Deloitte
- **Kevin Kozlowski**, XTec, Incorporated
- **Lolie Kull**, HP Enterprise Services
- **LaChelle LeVan**, Probaris
- **Diana Loughner**, IDenticard
- **Stafford Mahfouz**, Tyco Software House
- **Don Malloy**, NagraID Security
- **Debbie Marshall**, Smart Card Alliance
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, Identive Group
- **Roger Morrison**, Datacard Group
- **Rodney Pieper**, HP Enterprise Services
- **Zeca Pires**, Datacard Group
- **Rick Pratt**, XTec, Incorporated
- **Steve Rogers**, Intellisoft, Inc.
- **Abel Sussman**, Booz Allen Hamilton
- **Rick Uhrig**, XTec, Incorporated
- **Chris Williams**, SAIC
- **Mike Zercher**, NXP Semiconductors

The Smart Card Alliance also thanks **Duane Stafford**, Office of the Secretary of Veterans Affairs & Homeland Security, Commonwealth of Virginia, for comments and input on the Commonwealth of Virginia PIV-I FRAC case study.

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting best policies and practices concerning person and machine identity, including strong authentication and the appropriate authorization across different use cases. Through its activities the Council encourages the use of digital identities that provide strong authentication across assurance environments through smart credentials – e.g., smart ID cards, mobile devices, enhanced driver's licenses, and other tokens.

The Council addresses the challenges of securing identity and develops guidance for organizations so that they can realize the benefits that secure identity 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.

Trademark Notice