ENABLING SECURITY, COMPLIANCE AND EFFICIENCY:
Achieve Your Federal Identification Credentialing Goals
Identity management and verification depend on trusted credentialing technologies. U.S. federal, state and local governments and private enterprises alike are seeking ways to improve security, not just for facility access, but also for single-sign-on into cyberspace. Furthermore, non-federal issuers of identity cards demand cost-effective, compliant methods to produce identity cards that interoperate with federal government Personal Identity Verification (PIV) and PIV-Interoperable (PIV-I) systems.

Beyond government applications, the private sector also stands to gain from secure credentialing standards and technologies. The PIV-I card is a non-federally issued credential designed for use by state and regional employees, including first responders. The PIV-I card meets all FIPS 201 standards and is recognized and trusted by the federal government. PIV-I cards can provide states, local jurisdictions, and enterprises a single, interoperable, and secure credential usable across multiple application areas. The result is a more secure infrastructure, and better services for employees, contractors, businesses and consumers.

This white paper provides an overview of FIPS 201-compliant smart ID cards and shows the significant benefits the technology enables. The paper also shows how to produce PIV-I compliant access cards that contain tamper-resistant coatings, radio frequency identification (RFID), and other features using the latest printing technologies.

EXECUTIVE SUMMARY

INTRODUCTION—CREDENTIALING HAS STRICT REQUIREMENTS

Today’s threat-filled world calls for new methods to enhance security, increase efficiency, reduce identity fraud, and protect personal privacy. Finding a method to ensure the right person accesses only the information and facilities he or she is entitled to remains a top priority for both government and private industries. Whether it is protecting a cloud data center or single-sign on through the Web, enterprises require secure credentialing standards and a trusted, repeatable implementation framework.

On August 27, 2004, the U.S. government issued Homeland Security Presidential Directive 12 (HSPD-12) calling for identification standards for government employees and contractors. Since then, The National Institute of Standards and Technology (NIST) created the Federal Information Processing Standard Publication 201 (FIPS 201) for secure and reliable forms of identification. The FIPS 201 requirements for physical and logical access for federal employees and contractors are defined by the federally-issued PVI I and PVI II standards. Note that PVI refers to PIV-Interoperable, whereas PVI I and II refer to the actual background check, software, and hardware requirements.

Created initially in response to terrorist threats, HSPD-12 directs the use of a common identification credential for both logical and physical access to federal controlled facilities and information systems. HSPD-12 requires that the federal credential be secure and reliable. In support of HSPD-12, the FIPS 201 standard includes two stringent requirements: PIV I and PIV II.
The PIV I requirements define the control objectives and security requirements described in FIPS 201, including the standard background investigation required for all federal employees and long-term contractors. The standards in PIV II define the technical interoperability requirements described in FIPS 201. PIV II specifies the hardware implementation standards for implementing the identity credentials. This directly affects all smart cards designed for use in federal applications. FIPS 201 requires agencies to:  

- “Establish roles to facilitate identity proofing, information capture and storage, and card issuance and maintenance.”  
- “Develop and implement a physical security and information security infrastructure to support these new credentials.”  
- “Establish processes to support the implementation of a PIV program.”

Deployment of PIV is rapidly gaining momentum. In fact, the U.S. government has issued over 5 million FIPS 201 standard PIV cards to federal employees and contractors since 2005 in a wide range of trusted identity applications.

SMART CARDS AND PIV—WHAT YOU NEED TO CONSIDER

Most of today’s identification and badging systems depend on magnetic stripes, barcodes, or simple photographs. Newer, contactless identification badges integrate UHF radio frequency identification (RFID) technologies. While these approaches can associate the badge to the access point, they cannot verify that the right person is in possession of the badge. In most cases, these technologies cannot fulfill the requirement of delivering strong security while still guarding personal privacy. Traditional ID badges are tamper-prone, can be counterfeited easily, and provide insufficient protection for the card’s stored data.

When used in a properly implemented system, smart card IDs enable all the security features required to enhance privacy protection. Smart cards contain an embedded chip providing built-in tamper resistance along with memory to securely store data, execute logical functions, and interface with a smart card reader using barcodes, magnetic stripes, or contactless RFID technology. The result is an identity management system with strong information, privacy protection, and ID security.

In addition, the smart card’s embedded microprocessor enables encryption, decryption, and biometric matching for authenticating information access. When organizations choose smart cards, they can significantly expand privacy protection while verifying personal identity.

Multi-factor Authentication

PIV-compliant smart cards provide secure, multi-factor authentication at a high level of assurance. They combine a cryptographic private authentication with a personal identification number, fingerprint biometric template, and tamper-proof digital photograph. The security department issues the credentials after running a detailed background check on a person. When used with biometric technology, smart cards provide very high levels of assurance for confirming the person’s identity. Once the security department programs the smart card and associates it to the user, it provides a trusted identity usable for a wide range of cyber-based and physical access transactions.

Agencies and businesses planning to move to the PIV (or PIV-I Interoperable) standard should carefully consider each aspect of their infrastructure and security processes, from the smart card itself, to the card reader, to the security database. They also need to understand the PIV-I data model.
PIV-I Logical Data Model Requirements

FIPS 201 section 4.1.5.1 details the PIV-I Card logical data model definitions. To support a variety of authentication mechanisms, PIV-I card logical credentials contain multiple data elements for verifying the cardholder’s identity at graduated assurance levels and are mandatory. These include:

- Card Capability Container
- Cardholder Unique Identifier (CHUID)
- Logical authentication key that consists of one asymmetric key pair and a corresponding certificate
- Card authentication key that consists of one asymmetric key pair and corresponding certificate
- Two biometric fingerprints
- Facial image buffer
- Security object

In addition, the logical data model defines several optional elements that are extensible to meet application or organization-specific requirements. The optional elements include:

- Printed information buffer
- Discovery object
- Key history object
- Retired key management keys
- Digital signature key
- Key management key
- Symmetric key associated with the card management system

Once an organization deploys PIV-enabled smart cards, they can begin to realize the significant benefits the technology delivers. And this is in addition to simply meeting government or industry-mandated compliance initiatives.

TRUSTED IDENTITY ENABLES BENEFITS INDUSTRY-WIDE

The standards and best practices within FIPS 201 set the foundation for a wide range of applications for both industry and government. In fact, FIPS 201 leverages existing ANSI, ISO, IETF, and other highly proliferated standards that are critical to thousands of applications. As a result, most operating systems, mobile and enterprise applications, services, and physical access control systems automatically support PIV-I credentials.

Controlling Access to Facilities

Agencies from law enforcement, to emergency response, to federal entities can all benefit from FIPS 201. Secure access to facilities and cyber resources allows interoperability across multiple jurisdictions, strong proof of cardholder identity, and the ability to authenticate identity and attributes electronically. Adoption of FIPS 201 means that agencies only require the issuance of one ID, instead of multiple IDs. Doing so helps reduce redundant security credentialing efforts and expenditures, and increases security policy effectiveness.

In the private sector, PIV-I-enabled smart cards allow businesses to improve security at places of employment, restrict access to sensitive areas, and reduce incidences of theft. Most losses do not occur from overt break-ins or elaborate employee fraud schemes, but from simple crimes of opportunity. Ensuring that the right person has the right access to facilities, equipment, and supplies can prevent a significant amount of unauthorized activity.

Securing Cyberspace

With information security a top priority in both the public and private sector, FIPS 201 provides a trusted way for Web users to access information and purchase products and services online. Recently, the General Services Administration (GSA) implemented a co-op purchasing program for state and local governments. With FIPS 201 compliance in place, government workers can use their PIV-enabled smart cards to acquire products through the online GSA portal securely and cost-effectively.
Strong credentialing also protects against identity theft, reducing incidents of fraudulent benefit, entitlement, or service payments to individuals who misrepresent themselves. Financial institutions can ensure that their employees and customers are only accessing privileged information, while meeting compliance mandates.

Government agencies and private enterprises can use FIPS 201 credentialing to enable secure collaboration and information sharing between organizations including email, intellectual property, and personal information stored in human resources databases. Additionally, organizations can reduce physical paperwork and streamline processes by using digital signature technologies that authenticate each user.

PRINTING SOLUTIONS FOR FIPS 201-COMPLIANT SMART CARDS

Achieving FIPS 201-compliance requires that all processes and infrastructure align with requirements—which includes smart card printing technology. All smart card technologies described in this paper including barcode, RFID (contactless smart card), magnetic stripe, graphic, and photo security features, can be printed on demand at the user’s own facility, wherever and whenever. However, not all card printers are FIPS 201-compliant. The GSA operates independent testing procedures to validate and approve products that comply with FIPS 201 and publishes the results as a publicly accessible Approved Products List (APL).7

Smart Card Printers—Why They Are Critical

Digital-quality plastic card printers offer the ability to create custom cards tailored to the application, at the point of issuance. System administrators can invalidate lost or stolen cards and issue replacements immediately. Unlike traditional ID card systems that lacked customization or required time-consuming photo processing, cutting and laminating, today’s digital print-on-demand (POD) systems enable completely automated production of highly customized, secure cards. A wide variety of card printers exist to meet user needs, including high duty cycle models for applications that require thousands of cards annually.

Digitally printed smart cards provide numerous technological features, but start with a blank plastic card customizable with any combination of artwork, graphics, text, digital photographs, barcodes, logos and more. The printer can encode additional machine-readable information, such as magnetic stripes, RFID, and smart card chips. The image quality of plastic photo ID cards produced with digital printing technology is far superior and tamper-resistant compared to those produced through the traditional method of trimming printed photos and laminating them onto the card. Different card materials and laminates provide additional protection from tampering.

FIPS 201-compliant security-class card printers from Zebra allow agencies to print highly secure and durable ID cards. Designed for both the private and public sector, the FIPS 201-compliant8 Zebra ZXP Series 8™ laminating retransfer card printer delivers high throughput and print speed. On-demand printing of vivid color plastic cards helps increase operational efficiency without sacrificing image quality for a wide range of applications:

- Employee ID and access control cards
- Government-issued driver licensing
- High-security ID and access control cards
- Instant-issuance bank cards
- National ID and voter registration cards

Also approved as FIPS 201-compliant9, the Zebra P640i™ card printer supports dual-sided lamination and a wide range of tamper-resistant features for the highest-security applications including:

- Government-issueddriver licensing
- High-security access control and ID cards
- Government employee ID cards
- Secure airport ID cards
- Law enforcement/correctional facility ID cards
- National ID and voter registration cards
CONCLUSION

Interoperable trusted credentials are a cornerstone of security, both physical and cyber. Meeting the PIV-Interoperable, PIV I, and PIV II requirements as detailed in FIPS 201 moves agencies and organizations beyond simple access control into the sphere of trusted identity. Only the right person can access the right facility and information at the right time. Trusted identity establishes the identity of the cardholder, and only PIV-enabled smart cards can meet this standard.

Adopting PIV-enabled smart cards means that organizations can streamline their infrastructure while protecting information and personal identity. Private and public sector enterprises can meet the requirements for collaborating with federal government and relying parties. Secure, print-on-demand systems from Zebra enable completely automated production of highly customized, secure smart cards. Now, enterprises seeking to implement trusted identity applications can rest assured that each part of their infrastructure, including their printers, meets the most stringent requirements of FIPS 201.

A global leader respected for innovation and reliability, Zebra offers technologies that illuminate organizations’ operational events involving their assets, people and transactions, allowing them to see opportunities to create new value. We call it the Visible Value Chain.

Zebra’s extensive portfolio of marking and printing technologies, including barcode, RFID, GPS and sensing, turns the physical into the digital to give operational events a virtual voice. This enables organizations to know in real-time the location, condition, timing and accuracy of the events occurring throughout their value chain. Once the events are seen, organizations can create new value from what is already there.

For more information about Zebra’s solutions, visit www.zebra.com.

---

6 Ibid.
7 FIPS 201 Evaluation Program Approved Products List (APL), http://fips201ep.cio.gov/apl.php
8 Ibid.
9 Ibid.