

HSPD-12 & FIPS 201 PIV II: How Government Standards Affect Physical Access Control

HSPD-12—A Common Identification Standard for Federal Employees and Contractors

Homeland Security Presidential Directive 12 (HSPD-12) is a policy for a common identification standard for federal employees and contractors. It was written with a goal of creating secure and reliable forms of identification that are:

- Issued based on sound criteria for verifying an individual employee’s identity (including a full vetting procedure with specific processes for background check);
- Rapidly authenticated electronically via contact or contactless credentials;
- Issued only by providers whose reliability has been established by an official accreditation process; with
- Graduated criteria and different security levels, from least secure to most secure, to ensure flexibility in the identification process.

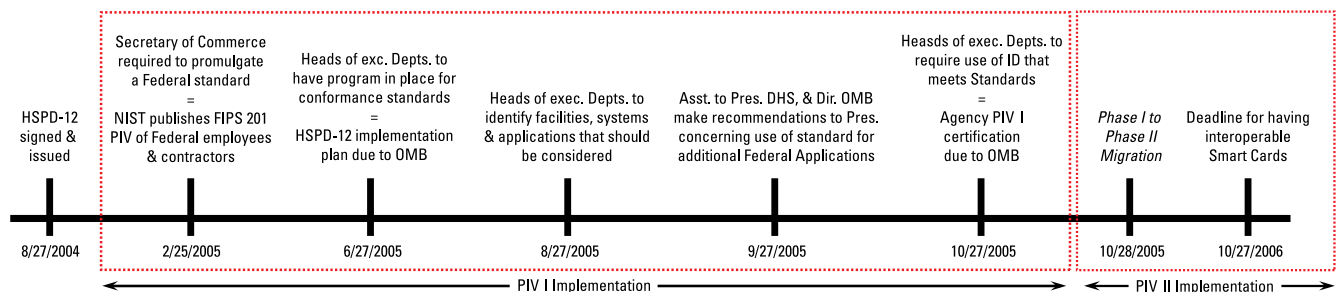
In response to HSPD-12, the National Institute of Standards and Technology (NIST) Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. Federal Information Processing Standard 201 (FIPS 201) was developed to satisfy the technical requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005. FIPS 201 specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors.

There is an abundance of material and information (presentations, white papers, FAQ’s) available regarding FIPS 201. The goal of this piece is to provide information about the differences between legacy access control technology and FIPS 201-mandated access control. In the process, some of the disadvantages related to using microprocessor based dual-interface cards for the same application are revealed.

It is important to understand that FIPS 201 was written to ensure cardholder identity during issuance and to leverage existing contact-based logical access applications; physical access was not the primary consideration of FIPS 201.

HSPD-12 Timeline

The Timeline for HSPD-12/FIPS 201



Source: DHS, NIST

The Differences between Legacy Access Control and FIPS 201

In looking at legacy access control systems and FIPS 201 mandated access control, the most evident differences are revealed by the user experience. Users of the FIPS 201 system generally will encounter a different user experience, decreased traffic throughput due to time considerations, issues with compatibility with Physical Access Control Systems (PACS), optional security depending on the level of access used, a different range of available applications based on the access control used, difficulty in finding available products with General Services Administration (GSA) approval and interoperability compatibility issues. Many of these issues are due to the rigidity of the mandated FIPS system, as opposed to the commercially available legacy access control systems.

Below, we provide a quick glance table highlighting the specific differences between legacy access control and FIPS 201 access control across a number of key parameters.

Specific Differences between Legacy Access Control and FIPS 201

	Legacy Access Control	FIPS 201
Read Range	Usually 3-8"; up to 2'	< 2"
Read Time	< 200 ms	> 700 ms
Format Length	< 40 bits	40 -200 bits (or larger)
Security	Broad range of security levels based on technology	Multiple levels of assurance
Other Applications	Biometrics, logical access, time & attendance, cashless vending & P.O.S., loyalty systems, medical record management, campus systems	Biometrics (via contact interface only)
Product Availability	Largely commercially available from several vendors	Limited, represents a sub-set of total product offerings
Product Interoperability	Open compatibility or "matched-set" card/reader compatibility	Maximum interoperability; users must be aware of configurable features across manufacturers

The following provides a more in-depth description of the specifics of the competing systems.

Read Range

Legacy Access Control

The communications protocol and power required to excite proximity and memory card technology chips allows read ranges from 3 to 8 inches at the door. Proximity technology also allows for extended read ranges, up to 2 feet with passive cards, for parking applications.

FIPS 201

FIPS 201 is based on the ISO14443 communication standard with dual-interface cards, which require additional power to excite the microprocessor. This tends to keep the read ranges under 2 inches in all environments.

Read Time

Legacy Access Control

Proximity (< 84 bits) and memory card (< 104 bytes) technologies transfer a small amount of data that needs to be processed after an almost instantaneous (< 200 ms) card-to-reader dialogue. The access control information (format) is usually stored in a default location that ensures immediate locating.

FIPS 201

FIPS 201 defines a file structure that must be addressed by the reader after a FIPS 140 cryptographic self-test (> 700 ms). Additionally, the access control information (FASC-N, expiration date, etc.) can be located anywhere within the CHUID (Card Holder Unique Identifier) file (3500+ bytes). This lengthened read time requires the user to hold the card steady in front of a reader, for an extended period of time, until audio and visual feedback is provided.

Format Length

Legacy Access Control

Most legacy access control systems have limitations to the length of specific fields, and the overall length of the unique identifier (format) that can be processed. Memory cards, like proximity, adopted the existing compatible formats that were less than 40 bits in length.

FIPS 201

The unique identifier for FIPS 201 is called the Federal Agency Smartcard Credential Number (FASC-N) and is 200 bits in length. The FASC-N is encoded on the card in accordance with ISO 7811, also known as standard magnetic stripe encoding. A portion of the FASC-N, the first three fields (40 bits), is an acceptable output, but the output can be much longer, particularly with the addition of the expiration date to the output, depending on the configuration of the reader and the needs of the system.

Security

Legacy Access Control

Proximity systems have limited security, although some incorporate password protection to achieve a higher security level. Memory cards use a sophisticated form of security utilizing mutual authentication and encryption.

FIPS 201

The FIPS 201 standard is written for maximum flexibility by allowing multiple levels of security, the lowest being a free read of the FASC-N. The medium assurance profile details additional security through the use of a Hashed Message Authentication Code (HMAC) calculation to protect the contents of the card from changing. The high assurance profile is still restricted to the contact interface of the dual-interface card.

Other Applications

Legacy Access Control

Some applications, like biometrics, are naturally suited for physical access control systems that require multi-factor authentication, but other applications like biometrics, logical access, time & attendance, cashless vending and P.O.S. (point-of-sale), loyalty systems, medical record management, campus systems and other special applications are becoming more prevalent. Proximity cards are used for lookup when the biometric template is stored in the reader, where memory cards primarily store the biometric template digitally on the card for instant one-to-one verification at the reader.

FIPS 201

FIPS 201 supports biometric verification for some applications, but it is restricted to the contact interface. There is currently no support for any other applications within a FIPS 201 credential.

Product Availability

Legacy Access Control

Legacy products are available in large quantities from a multitude of manufacturers through various channels

FIPS 201

A limited number of reader manufacturers have made the effort to support the FIPS 201 standard and they must submit their products to the GSA for evaluation and approval. Only those products that are listed on the GSA Approved Products List (APL) are available to be purchased under the GSA Schedule 70.

Product Interoperability

Legacy Access Control

Proximity and memory card technologies can be configured for open compatibility (any card works on any reader) or they can be configured as a matched set (only cards matching their reader equivalents will work).

FIPS 201

FIPS 201 was written to ensure maximum interoperability between the card and the reader, although care should be taken to ensure that readers purchased from multiple manufacturers have the same configurable features.

PIV Q&A

“How do we transition from our current legacy technology to FIPS 201?”

- | | |
|----------------|--|
| Cards | A proximity technology coil can be added to the dual-interface FIPS 201 credential. This multi-technology dual-interface credential will be available from multiple suppliers. |
| Readers | Only a few manufacturers offer multi-technology readers that have the capability to read legacy technologies and FIPS 201 credentials at the same time. |

All of the other parameters mentioned in this presentation must be addressed before attempting a transition.

Conclusion

The process for establishing the government standards is still evolving so it is our goal to provide some clear cut answers about this critical global standard. By learning about the differences between Legacy Access Control credentials and FIPS 201 access control, you can make more informed decisions in your organization’s stance toward FIPS 201. If you have further questions, or need more detail on any of the points raised within this document, please contact Nathan Cummings, Director of Product Management, HID Global Corporation (email: ncummings@hidcorp.com).

FIPS 201 Compatible Products from HID

Multi-Technology Readers

FIPS 201-certified with iCLASS® at the same time

R10



6100BKN0000-G3.0

R30



6110BKN0000-G3.0

R40



6120BKN0000-G3.0

RK40



6130BKN000000-G3.0

Multi-Frequency Multi-Technology Readers and Embedded Products

FIPS 201-certified with Prox (e.g., HID Prox and Indala® Prox) and iCLASS at the same time.

RP40



6125BKN0000-G3.0

OEM150



3121BNN0000-G3.0

Features

- ▶ +5 - 12 VDC
- ▶ < 100 mA Current Draw
- ▶ -40° F to 150° F
- ▶ Tamper Switch

Configurable Output for all FIPS 201-certified Readers

- ▶ Multiple FASC-N outputs from 40 to 200 bits
 - With or without parity, start/end sentinels, field separators
 - MSB or LSB first
- ▶ HMAC calculation for Medium Assurance Profile
 - CSN + Entire CHUID + SSK = 32 bit result
- ▶ Custom Outputs
 - 80 bit – Agency + System + Credential + HMAC (binary)
 - 75 bit – Agency + System + Credential + Expiration (binary)
- ▶ Any combination of FASC-N , CSN, and the other CHUID tags

Appendix I. Acronym Glossary

- ▶ APL – Approved Products List --GSA published list of FIPS 201 approved products
- ▶ CHUID – Card Holder Unique Identifier --One of many files contained in the FIPS 201 card
- ▶ FASC-N – Federal Agency Smartcard Credential Number --The government selected format stored in the CHUID
- ▶ FIPS – Federal Information Processing Standard
- ▶ GSA – General Services Administration --Provide the evaluation guidelines for FIPS 201 approval of products
- ▶ GSA Schedule 70 – A contract administered by the Federal Supply Service of the General Services Administration
- ▶ HMAC – Hashed Message Authentication Code --A hash function that uses a key
- ▶ HSPD-12 – Homeland Security Presidential Directive 12 -- a policy for a common identification standard for federal employees and contractors
- ▶ ISO – International Standards Organization --Details the contactless standards for communication w
- ▶ NIST – National Institute of Standards and Technology --Wrote FIPS 201 and evaluate the card applet for FIPS 140
- ▶ PACS – Physical Access Control System
- ▶ PIV – Personal Identity Verification Primary goal of FIPS 201 system
- ▶ PIV II – Technical and interoperability standards for Personal Identity Verification
- ▶ SSK – Site Specific Key

Appendix II. Other Sources of Information

- ▶ e-Authentication - <http://www.cio.gov/eauthentication>
- ▶ General Services Administration (GSA) - <http://www.smart.gov/>
- ▶ HID Global - http://www.hidcorp.com/page.php?page_id=59
- ▶ National Institute of Standards and Technology (NIST) - <http://csrc.nist.gov/piv-program/>
- ▶ Security Industry Association (SIA) - <http://www.siaonline.org/government/index.cfm>
- ▶ Smart Card Alliance (SCA) - <http://www.smartcardalliance.org/pages/publications-fips-201-resources>

Author: Nathan Cummings, Director of Product Management, ncummings@hidcorp.com, January 9, 2007