STANLEY®
Security

HSPD 12 & FIPS 201

TABLE OF CONTENTS

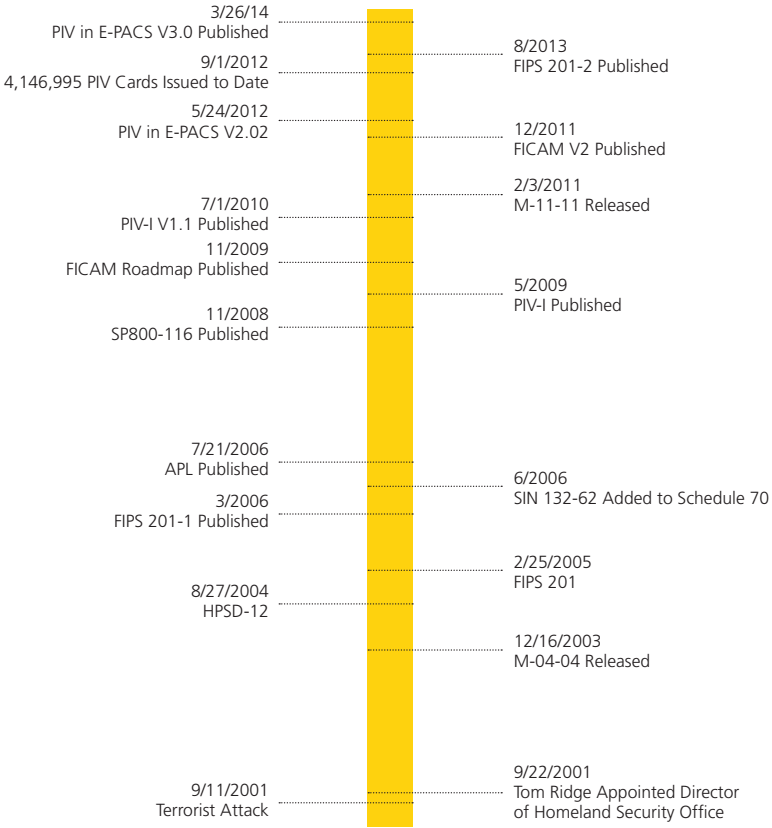
PURPOSE OF THIS DOCUMENT

This document is intended to provide a high level overview of the HSPD 12 directive, to give the reader a minimum understanding of the impact HSPD 12 has had/will have in the government electronic security vertical, and the electronic security industry as a whole.

Although the goal is to provide a fundamental understanding for those in the US government security field, it's assumed that the reader already has a working knowledge of electronic security and the US government.

Unless otherwise stated, the contents of this document apply only to the United States Federal Government under the Executive branch.

Please refer to the reference section in the back of this booklet for more detailed information.



Sequence of Events

BACKGROUND

The September 11 attacks were a series of four coordinated terrorist attacks launched by the Islamist terrorist group al-Qaeda upon the United States in New York City and the Washington, D.C. areas on September 11, 2001. On that Tuesday morning, 19 al-Qaeda terrorists hijacked four passenger jets, intending to fly them in suicide attacks into targeted buildings.

Two of those planes, American Airlines Flight 11 and United Airlines Flight 175, were crashed into the North and South towers, respectively, of the World Trade Center complex in New York City. Both towers collapsed within two hours and falling debris, combined with fires that the debris initiated in several surrounding buildings, led to the partial or complete collapse of all the other buildings in the World Trade Center complex, also causing major damage to ten other large structures in the immediate area of the complex.

A third plane, American Airlines Flight 77, was crashed into the Pentagon (the headquarters of the United States Department of Defense), leading to a partial collapse in its western side.

The fourth plane, United Airlines Flight 93, was targeted at the United States Capitol in Washington, D.C., but crashed into a field near Shanksville, Pennsylvania after its passengers tried to overcome the hijackers. Almost 3,000 people died in the attacks, including all 227 civilians and 19 hijackers aboard the four planes.

The 20th al-Qaeda terrorist had been denied access in Orlando by an immigration official in August just prior to the attacks.

All 20 attackers had valid, and in most cases several valid ID's.

New York City buildings were placed in lock down, and only those with valid credentials to the facilities access control system(s) were allowed access. External aid was denied access, and victims were left helpless because there was no way for individuals without local access cards, to be authenticated.

The pentagon was in lockdown, and because of an incident involving a photographer, the Arlington fire department was turned away. The Arlington police chief was denied access despite being crucial to the rescue effort.

September 11th and the series of events that followed made it very clear to the federal government, state and local governments, and officials that this nation seriously lacked the ability to properly identify, and thereby trust an individual to be who they say they are.

HSPD 12

Eleven days after the September 11, 2001, terrorist attacks, Pennsylvania Governor Tom Ridge was appointed as the first Director of the Office of Homeland Security in the White House. The office oversaw and coordinated a comprehensive national strategy to safeguard the country against terrorism and respond to any future attacks.

Beginning in October 2001, a series of Homeland Security Presidential Directive's (HSPD), were issued by the executive office under President George W. Bush. The first of which was issued on October 29th, 2001 which created the Homeland Security Council.

A full list of these directives can be found at the following link: http://www.epa.gov/homelandsecurityportal/laws-hspd.htm

Directive Twelve (HSPD 12) was created August 27th, 2004 and can be summed up in the following statement:

There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. To mitigate these threats HSPD 12 calls for: U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.

Full text of HSPD 12: DHS website: http://www.dhs.gov/homeland-security-presidential-directive-12

HSPD 12 specifies a secure and reliable means of identification that:

- Is issued based on sound criteria for verifying an individual employee's identity.
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.
- Can be rapidly authenticated electronically.
- Is issued only by providers whose reliability has been established by an official accreditation process.

As promptly as possible, but in no case later than eight months after the date of promulgation, executive departments and agencies are required to implement the standard for identification issued to Federal employees and contractors in gaining physical access to controlled facilities, and logical access to controlled information systems. The directive stipulated that the standard include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

The White House publishes a quarterly status report on HSPD 12 implementation for each agency and can be found here: http://www.whitehouse.gov/omb/e-gov/hspd12_reports

HSPD 12 prompted the National Institute of Standards and Technology (NIST) (under the Department of Commerce) to create the Federal Information Processing Standard known as FIPS 201, titled "Personal Identity Verification (PIV) of Federal Employees and Contractors." FIPS 201 was approved by the Secretary of Commerce, and issued on February 25th, 2005. The standard was effective immediately and gave federal agencies under the executive branch, until October 27th, 2005 to meet its requirements. In March 2006 the standard was updated with Change Notice 1 and finally with FIPS 201-2 in August 2013. The result of FIPS 201-2 created the PIV card currently being issued to all federal government employees and federal contractors (under contract for 6 months or more).

FIPS 201

FIPS 201-2 defines the architecture and technical requirements for HSPD 12.

Full text can be found here: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

Summary

FIPS 201 specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems.

In order to minimize risk of counterfeit or otherwise unauthorized PIV credentials being issued to unqualified or unverified persons, a procedure known as the PIV process was created. This process is outlined in PART ONE (I) of the FIPS 201 standard (Roman numeral one, not to be confused with the PIV-I (interoperable) card).

FIPS 201 Part One *describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12, including personal identity proofing, registration, and issuance.*

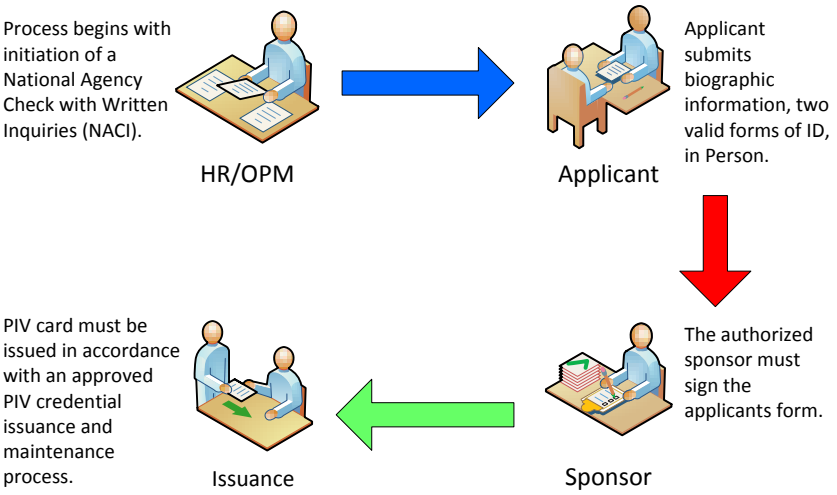


Figure 1 – PIV Part 1 (PIV-1) Process Summary

Figure 1 depicts at a high level the process by which an applicant (potential employee or government contractor) must complete in order to receive a PIV card. This process begins with the applicant being sponsored (not depicted) and submitting his/her application. The process is complete when final approval has been issued and the applicant receives her/his credential.

FIPS 201 Part Two *provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73, Interfaces for Personal Identity Verification. Similarly, the interfaces and data formats of biometric information are specified in Special Publication 800-76, Biometric Data Specification for Personal Identity Verification.*

This standard does not specify access control policies or requirements for Federal departments and agencies.

In order to meet the control objectives identified in FIPS 201-2 section 2.1, PIV Identity Proofing and Registration Requirements are outlined in section 2.7. These requirements help to minimize the risk of counterfeit PIV credentials. In short the process is as follows:

Sponsorship – an authorized sponsor within a federal agency must "sponsor" the individual applying for a PIV card.

Enrollment – the applicant enters in his/her biographic information.

Registration – the applicant shows up at an enrollment station/location and finishes the enrollment process with I-9 documents and biometric capture.

Background Check/Adjudication – utilizing biographic & biometric information (fingerprints) OPM/FBI performs an investigation.

Issuance – once approved the applicant shows up to an issuance station/location to receive, activate the card and load its certificates.

This process intentionally separates each role such that: no one person can fill more than one key roll in the process. For example the sponsor cannot also act as the enrollment officer, or the enrollment officer cannot act as the adjudicator or vice versa. This separation of rolls along with the process itself greatly reduces the risk of PIV cards being issued to unauthorized individuals.

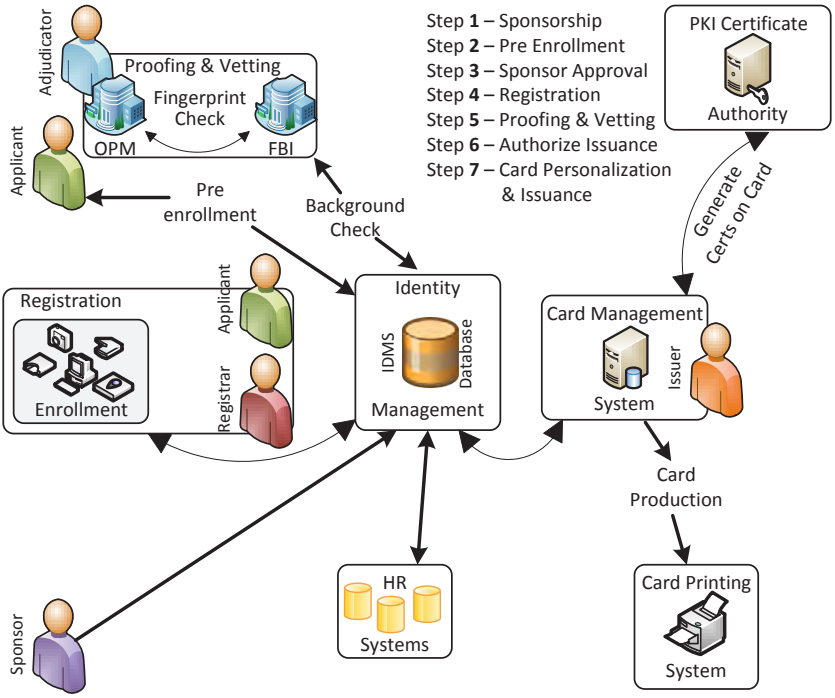


Figure 2 – PIV Card Issuance Components (Parts I & II)

Figure 2 summarizes the systems typically utilized in processing an application for a PIV card in the federal government. The figure also identifies the various individual roles (trained & certified) required in the process.

These roles are as follows:

Applicant – The person applying to receive a PIV Card.

Sponsor – The trained and certified agency representative sponsoring the applicant.

Registrar – The certified government representative who verifies and captures the applicant's information.

Adjudicator – The certified government representative who is responsible for processing and making any final decision on the applicant's background check.

Issuer – The certified government representative that will issue the actual card to the applicant.

FIPS 201-2 is supported by the 800 series of NIST Special Publications that further define the technical requirements, some of which are listed here.

SP800-73 (SP800-73-3) Interfaces for Personal Identity Verification –

Part 1: End-Point PIV Card Application Namespace, Data Model and Representation.

Part 2: End-Point PIV Card Application Card Command Interface.

Part 3: End-Point PIV Client Application Programming Interface.

Part 4: Interfaces for Personal Identity Verification.

SP800-73-4 Interfaces for Personal Identity Verification –

Part 1: PIV Card Application Namespace, Data Model and Representation.

Part 2: PIV Card Application Card Command Interface.

Part 3: PIV Client Application Programming Interface.

SP800-76 (SP800-76-2) Biometric Data Specification for Personal Identity Verification.

SP800-78 (SP800-78-3) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (SP800-78-4 Revision in Process)

SP800-87 (SP800-87-Rev1) Codes for Identification of Federal and Federally-Assisted Organizations.

SP800-116 (Revision in process) A Recommendation for the Use of PIV Credentials in Physical Access Control Systems.

PIV CREDENTIAL

The Personal Identity Verification (PIV) card is a result of HSPD 12/FIPS 201, in both the process of proofing/establishing the identity and the credential or smartcard itself. This is the credential or PIV (Personal Identity Verification) credential currently being issued to federal employees and government contractors of 6 months or greater.

It's important to note, that the PIV card is not the only credential being issued within the federal government. The Department of Defense (DoD) issues what is known as the Common Access Card (CAC), which in addition to the CAC applet, also contains most of the electrical characteristics of the PIV card. The CAC carries a CAC applet, as well as the PIV applet. The Transportation Security Administration (TSA) issues what is known as the Transportation Worker Identification Credential (TWIC) card. Which not unlike the CAC, has most of the electrical characteristics of the PIV card. The TWIC carries a TWIC applet, as well as the PIV applet within the smart chip. Some examples are shown in Figure 3.

Figure 3 – Example (Left to Right) TWIC - CAC - PIV Cards

The intelligence community issues a credential known as the IC1 Badge or One Badge, which is not related to the PIV card. National Security Systems are exempt from HSPD 12 due to their sensitive nature thus the IC1 is not PIV compliant.

The PIV credential can only be officially issued by a federal agency. However, the value of the PIV, its established chain of trust, and integration with the federal government's trusted cryptographic infrastructure (commonly referred to as the Federal PKI Bridge), has generated a great deal of interest outside of the federal government.

The following describes at a high level the electrical characteristics of the PIV card and some use cases. However, as you will read in a later portion of this document, in an effort to properly authenticate the credential itself, changes are being made to increase the level of confidence when using the PIV card for physical access.

Generally speaking, the PIV card like any ID card is issued in order to allow the card holder, the ability to prove their identity. The most common method is by showing an authorized person your ID, that person would then look at the physical characteristics of the card to determine its authenticity.

In addition to the defined physical characteristics, the PIV card also contains a chip (making it a smart card) that contains elements of the cardholder's identity as well. Some of these elements are listed below.

Card Holder Unique Identifier (CHUID) – is used as a unique identifier made up of several data elements and digitally signed by the issuer of the credential. Some of these data elements include: (also see figure 4)

- Federal Agency Smart Credential Number (FASC-N)
- Global Unique Identification Number (GUID)
- Expiration Date

Digital Certificates – The PIV card can have several digital certificates generated and stored on the card. These include:

- X.509 Mandatory Certificate for PIV Authentication (aka PIV Auth)
- X.509 Mandatory Certificate for Digital Signature
- X.509 Mandatory Certificate for Key Management
- X.509 Mandatory Certificate for Card Authentication (aka CAK Auth)

Cardholder Fingerprints – Two minutiae templates representing primarily the left & right index fingers.

Cardholder Facial Image – A mandatory electronic facial image used for printing facial image on the card as well as for performing visual authentication during card usage.

Printed Information – The biographic information that is printed on the card itself. (Name, DOB, Hair Color, Eye Color, etc.)

Cardholder Iris Images – Used for Iris recognition. (optional)

Inclusion of Universally Unique IDentifiers (UUIDs) – A mandatory UUID, for cards issued by Non-Federal Issuers. (See PIV-I for more information)

With the chip in place and the minimum data elements encoded, authenticating the credential can go beyond the standard visual inspection, and be electronically authenticated with logical and physical access control systems.

The digital certificate (known in short as the PIV AUTH CERT) is the certificate used for logical access. This requires a PIN to be entered by the user to authorize access to the certificate on the card. For physical access the credential may or may not require a PIN depending on the level of security required for access.

The PIV card (in addition to meeting HSPD 12 directives) is designed to replace the common cards used in physical access control systems (PACS) such as Proximity, iClass, etc. The PIV card has both a contactless interface operating at 13.56 MHz in accordance with the ISO 14443 standard, and a contact interface operating in accordance with the ISO 7816 standard.

In summary, HSPD 12 directed NIST to create the FIPS 201 standard which generated several technical standards (Special Publication 800 series). With these standards the federal government now has a highly secure, electronically authenticatable token which can be trusted to help prove the identity of a government representative (the PIV card).

The PIV card's wireless antenna allows for contactless communication to the chip and its uniquely identifiable information making it practical for electronic access control.

APPROVED PRODUCTS LIST

As a part of the HSPD 12 government program GSA recognized that federal agencies would need assistance and guidance in selecting components (hardware, firmware and software) that were capable of supporting the FIPS 201 specification.

Additionally, these component manufacturers would need the means to test their products against the NIST standard and actual PIV Cards. This caused GSA to create what is known as the Approved Products List (APL). Manufacturers and providers are required to get their products on the APL in order to be considered a HSPD 12 compliant product, as applicable.

The APL can be found here: http://fips201ep.cio.gov/apl.php

Furthermore a new SIN (132-62) was added to GSA schedule 70 to accommodate HSPD 12 related products and services.

GSA Schedule 84, along with Schedule 70, coupled with the approved products list provide federal agencies a high degree of confidence that security systems they purchase will be HSPD 12 compliant. (Note: Schedule 70 and 84 are being revised to accommodate changes brought on by HSPD 12)

USAGE

With the majority of federal employees now having a PIV card, the next step in the process is using the credential.

Using the PIV Card to authenticate an identity in today's PACS generally means presenting the card to an APL listed reader, connected to an access control system capable of reading the CHUID, or the GSA 75-bits comprised of the first 48-bits of the FASC-N and the expiration date in the CHUID. Formats such as these are referred to as a FASC-N ID (FASC-N Identifier), to differentiate it from the full FASC-N.

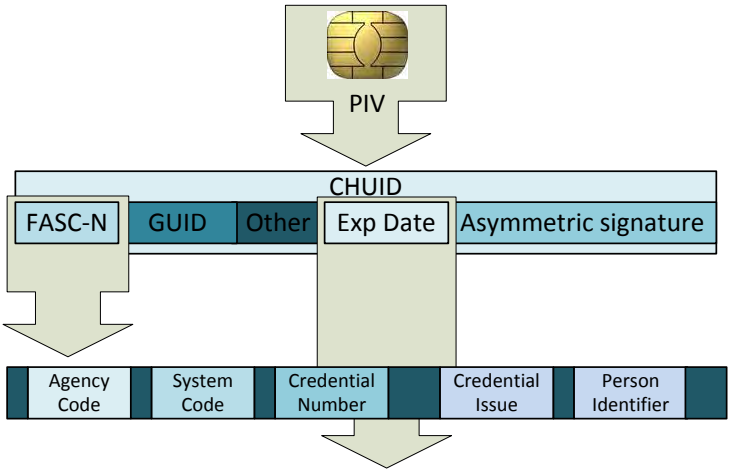


Figure 4 – Relevant data fields of the CHUID and FASC-N are shown

Figure 4 indicates that the CHUID is simply a data field stored inside of the chip on the PIV card, and that inside of the CHUID is the FASC-N. Within the FASC-N are the data fields that make up the unique identifier used for electronic access control.

[Note] Access control readers today output either the GSA-75 bit, or the full 200 bit FASC-N. Although this is the primary means of authenticating a PIV card in today's PACS, it provides no level of assurance that the card being read has not been spoofed or otherwise copied.

FIPS 201 describes three levels of assurance that can be correlated to three factors in the authentication process. These Assurance Levels are:

> **SOME Confidence** – A basic degree of assurance in the identity of the cardholder.
> **HIGH Confidence** – A strong degree of assurance in the identity of the cardholder.
> **VERY HIGH Confidence** – A very strong degree of assurance in the identity of the cardholder.

It's commonly accepted that these levels of assurance directly correlate to one factor, two factor and three factor authentication mechanisms.

Authentication Level	Factor
Single Factor (1)	Something you have- the card
Dual Factor (2)	Something you have, and something you know- the PIN
Three Factor (3)	Something you have, you know, and something you are- your fingerprint

Single Factor – Authentication consists of reading the minimum 48-bit FASC-N ID, GSA 75-bit FASC-N ID, or the full 200-bit FASC-N; either via the contact or contactless card interface. Special consideration has to be taken into account when dealing with cards other than the PIV card itself. For example the CAC leverages portions of the FASC-N that are only available when reading the full 200-bits.

Dual Factor – Authentication consists of reading either the FASC-N ID (48-bit or 75-bit) or the full 200-bit FASC-N, and the card PIN (contact only) or the PACS PIN (contact or contactless).

Three Factor – Authentication consists of the first factor, the second factor in contact mode only with the card PIN to unlock the biometric (fingerprint), and matching the fingerprint on the card or on the reader with the finger presented to the reader.

Simply reading elements of the CHUID such as the FASC-N is considered little-no confidence, and another authentication mechanism has been mandated to provide a higher level of assurance.

SP800-116

SP800-116 – A recommendation for the use of PIV Credentials in Physical Access Control Systems (PACS) was published November 2008 to provide guidance for federal agencies and the industry. Full text: http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

From the NIST SP800-116 document: *A gap remains, however, between the concepts of authentication assurance levels and their application in a PACS environment. To close this gap, this document:*

- *Discusses the different PIV Card capabilities so that the risk-based assessment can be aligned with the appropriate PIV authentication mechanism.*
- *Introduces the concept of "Controlled, Limited, Exclusion" areas to employ risk-based PIV authentication mechanisms for different areas within a facility.*
- *Proposes a PIV Implementation Maturity Model (PIMM) to measure the progress of facility and agency implementations.*
- *Recommends to Federal agencies an overall strategy for the implementation of PIV authentication mechanisms with agency facility PACS.*

Since the areas accessible via different access points within a facility do not all have the same security requirement, the PIV authentication mechanisms should be selected to be consistent with, and integral to, the overall security requirements of the protected area. A given facility may need multiple authentication mechanisms.

The document further goes on to introduce the designation of "Controlled, Limited, & Exclusion" areas and assigns a graduated number of authentication factors for each:

Security Area	Number of Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

The document continues and introduces the PIV Implementation Maturity Model (PIMM) which identifies levels of maturity of PIV Usage based on how many access points the PIV credential is leveraged versus non PIV usage. The levels are defined as follows:

Maturity Level 1 *– Ad hoc PIV verification.*

Maturity Level 2 *– Systematic PIV verification to Controlled areas. PIV Cards and currently deployed non-PIV PACS cards are accepted for access to the Controlled areas at this level.*

Maturity Level 3 *– Access to Exclusion areas by PIV or exception only. Non-PIV PACS cards are not accepted for access to the Exclusion areas at this level.*

Maturity Level 4 *– Access to Limited areas by PIV or exception only. Non-PIV PACS cards are not accepted for access to the Limited or Exclusion areas at this level.*

Maturity Level 5 *– Access to Controlled areas by PIV or exception only. Non-PIV PACS cards are not accepted for access to any areas at this level.*

Additionally SP800-116 references OMB M-04-04 – E-Authentication guidelines for Federal Agencies & SP800-63 – Electronic Authentication Guideline, which defines Assurance Levels 1 through 4 as follows:

Level 1: *LITTLE OR NO confidence*

Level 2: *SOME confidence*

Level 3: *HIGH confidence*

Level 4: *VERY HIGH confidence*

SP800-116 suggests a contactless authentication mechanism defined in SP800-73 known as 'Card Authentication Key (CAK)' pronounced "cake" so as not to be confused with 'CAC'. Prior to SP800-116, most if not all PACS were focused on reading the contactless CHUID. Where higher levels of confidence were needed, additional factors were added at the reader to verify the PIN, and possibly the cardholders fingerprint.

However in order for these additional factors (PIN & BIO) to be trusted, one must first trust that the card has not been duplicated or otherwise reproduced by an unauthorized entity. It would take little effort for a skilled individual to contactlessly read the CHUID from the PIV card of a federal employee, take that CHUID and produce another PIV card using the same CHUID, and THAT individuals PIN & BIO.

Should this unauthorized individual use this counterfeit card on the three factor reader, he/she would know the PIN and have a matching fingerprint. Because the CHUID is the only element used to make the access control decision, and the reader is telling the PACS that the PIN & BIO match; the duplicate PIV card grants the unauthorized individual access. SP800-116 authentication of certificates specifically address this vulnerability.

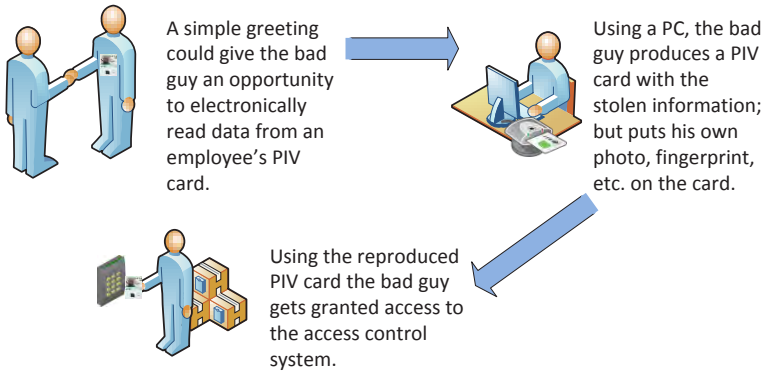


Figure 5 – PIV card data theft

In Figure 5, we see an example of one possible method that an unauthorized skilled individual could gain access to a federal facility with minimal effort. Because the bad guy is using the unique identifier stolen from the government employee, the access control system doesn't know that it's not the original PIV card being presented.

In order to better understand the complexity here let's digress a bit from our timeline and discuss Public Key Infrastructure (PKI), Digital Certificates (CERTS), and how they are used on the PIV card (in accordance with SP800-73).

PKI, CERTIFICATES AND THE CHALLENGE-RESPONSE REQUIREMENT

PKI is an extensive topic which will not be covered here in any broad manner. However in order to understand why SP800-116 is so important to the security industry, it's better to understand a few fundamental points.

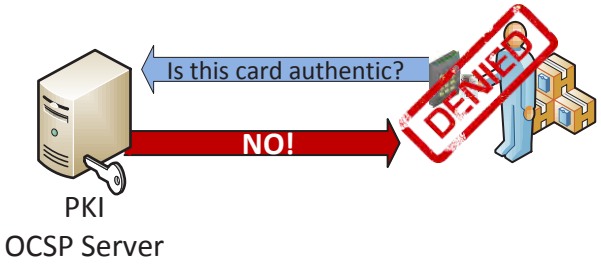
PKI is a form of cryptography in which two mathematically equivalent keys are used to encrypt and decrypt digital information. The infrastructure allows the use of what's known as a key pair, of which one key is public and provided freely with little to no restrictions; and the other key is private and securely protected (by the chip on the card in the case of PIV). Leveraging PKI allows for a highly secure method of authenticating a credential via an electronic method known as Challenge & Response. Although both keys are stored on the card, only the public key can be read, which is packaged in a file format known as a digital certificate or cert for short.

In the case of a SmartCard or more importantly the PIV SmartCard, these certificates which contain the public key, which is paired with the securely stored private key. When asked, the PIV card will provide the public key in the form of a cert, however it will not give up its private key.

Should someone want to verify that the card is authentic, one need only use the public key to challenge the card. Because only the card containing the private key, is capable of responding correctly, a valid response provides a very high degree of confidence in the cards authenticity. Additional processes take place to validate the public key and its authenticity, as well as ensuring the key pair can be trusted. This is an obvious over simplification, as there are many other factors and processes that take place for this authentication method to be performed, most of which are not within the scope of this document.

Up until now the majority of PACS used a contactless reader to extract a pseudo unique number from a card, because this number was given freely from the card when asked; its easily duplicated thereby providing little to no assurance that the card has not been copied from another valid source. This poses a high security risk when the credential or card is being used to access increasingly more secure areas of federal facilities. By leveraging the PKI standard and giving the card a private key that only it contains, it allows the reader to challenge the card in order to verify the card is authentic and not a reproduction or duplicate.

Now let's get back to our example of the so called 'unauthorized individual.' Should this counterfeit card be presented to the same 3 factor reader, with the ADDED benefit of a CAK authentication process; the reader now has a means in which to challenge the card's authenticity. Should the card prove not to be authentic, then no access is granted regardless of the CHUID's validity in the PACS.



Using the reproduced PIV card the bad guy gets DENIED access to the access control system.

Figure 6 – CAK or PKI Authentication

Figure 6 picks up from figure 5 indicating that with the added feature of PKI, the bad guy cannot create a duplicate PIV card that will gain access to a federal facility.

[Note] Although technically inaccurate, this authentication mechanism is often referred to as "going back to the federal bridge." Thus when someone says that they need a reader that goes back to the federal bridge, what they often are referring to is, a PKI or in this case a CAK authentication reader.

Thus far we have covered the WHY HSPD 12 exists. We've covered the WHAT HSPD 12 is. We've looked at the HOW HSPD 12 is implemented in the FIPS 201 specification document; we then gained some insight into the PIV card itself. And finally, discussed the now mandatory PKI authentication methods covered in SP800-116, as well as the associated benefits to PKI authentication.

The next sections will introduce the PIV-I card, FICAM, and PIV in E-PACS documents.

PIV-I

In May 2009 the Federal CIO council issued the Personal Identity Verification (PIV) Interoperability for Non-Federal Issuers document. PIV-I was updated July 2010 to version 1.1.

Full Text: http://www.idmanagement.gov/personal-identity-verification-interoperability

As the Personal Identity Verification (PIV) initiative progresses, it is garnering a great deal of interest from parties external to the Federal government. These non-federal organizations want to issue identity cards that are (a) technically interoperable with Federal government PIV systems, and (b) issued in a manner that allows Federal government relying parties to trust the cards. Furthermore, such interoperability and trust may be driven by operational imperatives of great interest to the Federal government (e.g. First Responder Authentication Credential (FRAC)). However, the PIV card standard, Federal Information Processing Standards (FIPS) 201, is limited in scope to the Federal government and has several requirements that can be addressed only by the Federal government community. Therefore, some guidance is needed to assist non-federal issuers of identity cards in achieving interoperability with Federal government PIV systems. This document provides that guidance.

This document advocates a set of minimum requirements for non-federally issued identity cards that can be trusted by the Federal government, and details solutions to the four barriers to interoperability that currently preclude Federal government trust of non-federally issued identity cards. These four barriers are as follows:

> ***Common terminology for identity cards** – in order to ensure consistency, a lexicon for differentiating a Federal government PIV card from a non-federally issued identity card seeking PIV system interoperability must be developed;*
>
> ***Technical requirements** – for non-federally issued identity cards to interact with federal infrastructure, basic technological requirements must be met;*
>
> ***Identifier namespace** – effective use of identity cards requires an identifier that is unique across all identity cards. Lack of a unique identifier may result in incorrect access control decisions; and*
>
> ***Trusted identity** – the fundamental purpose of an identity card is to establish the identity of the card holder. Therefore, an identity card must be issued in a manner that provides Federal government relying parties with a requisite level of trust.*

The PIV-I specification document defines a technologically interoperable credential, known today as simply the PIV-I card.

Although the PIV-I card is intended for use by non-federal personnel, some agencies are leveraging the credential for applications such as temporary access or visitor use cases.

Only the PIV card is issued by federal issuers, for employees and contractors 6-months and greater. Therefore, the PIV is for use by federal agencies, and to those they are allowed to issue them to, but it does not prevent these organizations from issuing PIV-I credentials for those that are not employees, but where access is allowed (approved visitors or contractors less than 6-months).

Furthermore the PIV-I card is being leveraged for programs such as the FRAC (First Responder Authentication Credential), and other programs by federal, state, local, and those actively doing business with the US federal government.

The PIV-I specification with some minor deviations, also has applications outside of government. In October 2011 the Smart Card Alliance Physical Access Council released a white paper describing what is known as the Commercial Identity Verification (CIV) Credential. The full text of which can be found here: http://www.smartcardalliance.org/resources/pdf/CIV_WP_101611.pdf

From an access control prospective the PIV-I credential differs from a federally issued PIV in that the FASC-N is not used as the unique identifier. The PIV-I uses the 128-bit Universally Unique Identifier (UUID).

FICAM ROADMAP

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance was originally released November 2009 (Version 1) and updated in December 2011 (Version 2) by the Federal CIO Council.

The full text can be found at the following location: http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202_0.pdf

A summary document (FICAM in Brief) provided by the Smart Card Alliance can be found here: http://www.smartcardalliance.org/resources/pdf/FICAM_Summary_20100514.pdf

The purpose of this document is to provide agencies with architecture and implementation guidance that addresses existing ICAM concerns and issues they face daily. In addition to helping agencies meet current gaps, agencies stand to gain significant benefits around security, cost, and interoperability which will have positive impacts beyond an individual agency in improving the delivery of services by the Federal Government. It also seeks to support the enablement of systems, policies, and processes to facilitate business between the Government and its business partners and constituents. The benefits associated with implementation of ICAM are summarized below:

Increased security, *which correlates directly to reduction in identity theft, data breaches, and trust violations. Specifically, ICAM closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing.*

Compliance with laws, *regulations, and standards as well as resolution of issues highlighted in GAO reports of agency progress.*

Improved interoperability, *specifically between agencies using their PIV credentials along with other partners carrying PIV-interoperable3 or third party credentials that meet the requirements of the federal trust framework. Additional benefits include minimizing the number of credentials requiring lifecycle management.*

Enhanced customer service, *both within agencies and with their business partners and constituents. Facilitating secure, streamlined, and user-friendly transactions – including information sharing – translates directly into improved customer service scores, lower help desk costs, and increased consumer confidence in agency services.*

Elimination of redundancy, *both through agency consolidation of processes and workflow and the provision of government-wide services to support ICAM processes. This results in extensibility of the IT enterprise and reduction in the overall cost of security infrastructure.*

Increase in protection of Personally Identifiable Information (PII) *by consolidating and securing identity data, which is accomplished by locating identity data, improving access controls, proliferating use of encryption, and automating provisioning processes.*

These benefits combine to support an improvement in the cyber security posture across the Federal Government with standardized controls around identity and access management. The ICAM target state closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. Leveraging the digital infrastructure in a secure manner will enable the transformation of business processes, which is vital to the future economic growth of the United States.

This document presents the Federal Government with a common framework and implementation guidance needed to plan and execute ICAM programs. While progress

has been made in recent years, this document is a call to action for ICAM policy makers and program implementers across the Federal Government to take ownership of their role in the overall success of the federal cyber security, physical security, and electronic government (E-Government) visions, as supported by ICAM. The Transition Roadmap and Milestones presented in Chapter 5 outlines several new agency initiatives and numerous supporting activities that agencies must complete in order to align with the government-wide ICAM framework, which is critical to addressing the threats and challenges facing the Federal Government.

PIV IN E-PACS

PIV in E-PACS (Current Version 3.0) - Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS) (Full Text: http://www.idmanagement.gov/sites/default/files/documents/Personal%20Identity%20Verification%20in%20Enterprise%20Physical%20Access%20Control%20Systems.pdf

The sole purpose of this document is to provide detailed technical and security guidance for leveraging PIV and PIV-I authentication mechanisms in a federal agency PACS - to provide interoperability across the federal enterprise and thus comply with directives such as [OMB M-11-11 – Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors].

The primary audience for this guidance is technical staff with responsibilities such as integrating PACS components, selecting PACs solutions, and determining the most appropriate local use of PIV and PIV-I in a local PACS.

A secondary audience is procurement officials that need technical guidance for citation in PACS procurements that intend to implement the mandates within [OMB M-11-11].

Produced by the Federal CIO Council, this draft Enterprise PACS guidance document is a look into the next level of paradigm shifts that HSPD 12 and FIPS 201 initiated. We now see the Approved Product List (APL) Program expanding to include larger components, making up the systems or solutions where previously only the peripheral devices were considered. Entire Physical Access Control Systems are being vetted and certified as compliant with the processes and components associated with the PACS use cases, as defined by the Federal Identity Credential and Access Management Initiative (FICAM).

GLOSSARY OF TERMS

Applet – A very small application, esp. a utility program performing one or a few simple functions. In this context "applet" refers to an application present or loaded onto a smart card chip.

Card Authentication Certificate – Also referred to as the Card Authentication Key or CAK (Pronounced: "Cake"), this is one of the mandatory digital certificates put onto the PIV Card.

Certificate Authority – In cryptography, certificate authority, or certification authority, (CA) is an entity that issues digital certificates.

Digital Certificate – In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document that uses a digital signature to bind a public key with an identity – information such as the name of a person or an organization, their address, and so forth.

Electrical characteristics – The applications and data available in the chip on a PIV / Smart card.

Federal PKI Bridge (Federal Bridge) – Bridges 3rd Party CA's to the Federal PKI common policy in order to establish a chain of trust. More commonly (although incorrectly) the term is used to describe PIV cards that are issued with certs, that have a trusted path back to the Federal Bridge CA.

PIV Authentication (PIV AUTH) Certificate – Also referred to as the PIV Auth Cert, is the key identify certificate and one of four mandatory certificates put on the PIV card today.

SmartCard – or integrated circuit card (ICC) is any pocket-sized card with embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethylene terephthalate based polyesters, acrylonitrile butadiene styrene or polycarbonate.

Public Key Infrastructure – A computerize form of message encryption using two keys (small files); one is public and used by the sender to encrypt the message, the other is private and used by the recipient to decrypt the message.

ABBREVIATIONS

APL – Approved Products List
CAC – Common Access Card
CAK – Card Authentication Key (Pronounced: "Cake")
CHUID – Card Holder Unique Identifier
DoD – Department of Defense
FAR – Federal Acquisitions Regulation
FASC-N – Federal Agency Smart Credential Number
FICAM – Federal Identity, Credential, and Access Management
FIPS – Federal Information Processing Standard
FRAC – First Responder Authentication Credential
GSA – General Services Administration
HSPD – Homeland Security Presidential Directive
NIST – National Institute of Standards and Technology
OCSP – Online Certificate Status Protocol
OMB – Office of Management and Budget
PIV – Personal Identify Verification
PIVAUTH – PIV Authentication Certificate
PIV-I – PIV Interoperable
SCA – Smart Card Alliance
SP – Special Publication
TWIC – Transportation Workers Identification Credential
UUID – Universally Unique Identifier

REFERENCES

Parts of this document were assembled from some of the following sources.

CIV Card – http://www.smartcardalliance.org/resources/pdf/CIV_WP_101611.pdf

Complete HSPD list – http://www.epa.gov/homelandsecurityportal/laws-hspd.htm

The DHS Website – http://www.dhs.gov/creation-department-homeland-security

DoD CAC Website – http://www.cac.mil/

FICAM Roadmap – http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202_0.pdf

FIPS 201-2 – http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

GSA APL – http://fips201ep.cio.gov/apl.php

HSPD 12 – http://www.dhs.gov/homeland-security-presidential-directive-12

HSPD 12 Implementation Information – http://www.whitehouse.gov/omb/e-gov/hspd12_reports

ISO 7816 – http://en.wikipedia.org/wiki/ISO/IEC_7816

ISO 14443 – http://en.wikipedia.org/wiki/ISO/IEC_14443

OMB M-04-04 – http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

OMB M-11-11 – http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

PIV-I for Non-Federal Issuers – http://www.idmanagement.gov/personal-identity-verification-interoperability

PIV in E-PACS – http://www.idmanagement.gov/documents/piv-e-pacs

SP800-63-2 – http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

SP800-73 – http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf

SP800-76-2 – http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf

SP800-78-3 – http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf

SP800-87-1 – http://csrc.nist.gov/publications/nistpubs/800-87-Rev1/SP800-87_Rev1-April2008Final.pdf

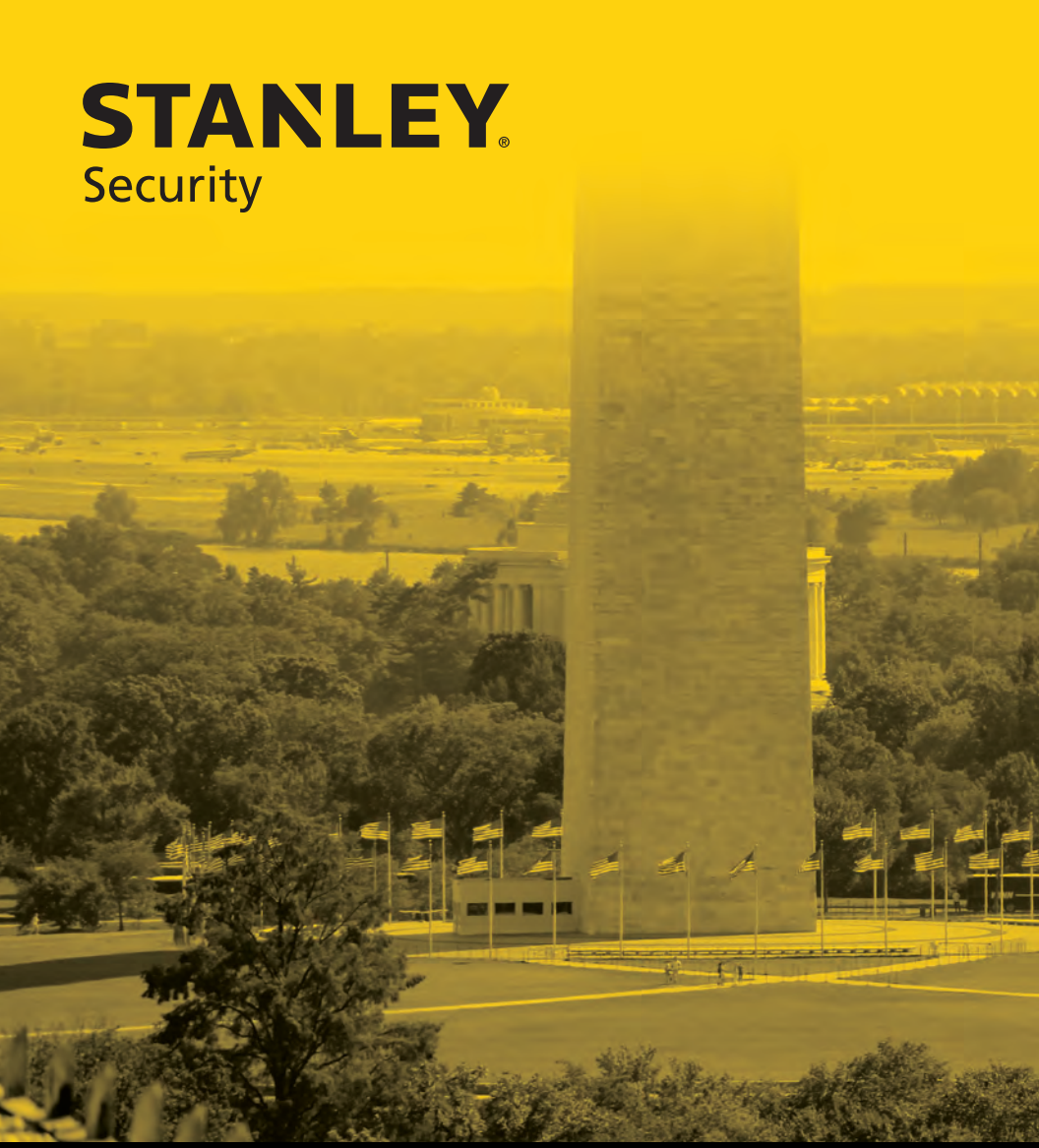
SP800-116 – http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

SCA FICAM Summary – http://www.smartcardalliance.org/resources/pdf/FICAM_Summary_20100514.pdf

The TSA (TWIC) Website – http://www.tsa.gov/for-industry/twic

Wikipedia – http://en.wikipedia.org

STANLEY®
Security



ABOUT US

STANLEY Security, a division of STANLEY Black & Decker (NYSE: SWK), is a provider of integrated security solutions for government, commercial and industrial organizations globally. We deliver a comprehensive suite of security products, software and integrated systems with a strong emphasis on service.

Learn more about how STANLEY Security can help meet your government security needs.

855-8-STANLEY | www.stanleycss.com/government

© 2015 STANLEY Convergent Security Solutions, Inc. and STANLEY Black & Decker Canada Corporation. All rights reserved. Any information that is made available by STANLEY Convergent Security Solutions, Inc. ("STANLEY") is the copyrighted work of STANLEY and is owned by STANLEY. THIS CONTENT IS PROVIDED AS IS, WITHOUT WARRANTY OF ANY KIND. Any use of the information contained herein is at the risk of the user. STANLEY does not assume the responsibility to update or revise content as new information becomes available. Visit www.stanleycss.com/licenses.html for licensing information. Version 1.5. 00357