Personal Identity Verification Card

By this time, Executive Branch agencies and departments should have the Personal Identity Verification (PIV) part I processes defined and in place. This paper focuses on the PIV technology and how the card interfaces to the outside. The challenge for Executive branch agencies and departments now is to implement the Part II requirements consistent with the Office of Management and Budget (OMB) guidelines. Personal Identity Verification has three functional areas: the front end subsystem; card issuance and management subsystem; and the access control subsystem. The PIV card and support infrastructure can be viewed from several vantage points including the life cycle and functional area. Requirements from the Federal Information Processing Standard (FIPS) 201 relating to the PIV card are discussed. This paper consolidates information from a number of sources and is limited to the PIV card, its interfaces, modes of authentication, and how it relates to e-Authentication.

1 What is a PIV Card?

The PIV card is a Polyvinyl Chloride (PVC (plastic)) credit card sized badge that contains a contact and contactless chip (or one chip implementing both technologies). By definition, a smartcard has embedded microelectronics. Thus, the contact and contactless chips can each be considered a smart card chip. The cards comply with a number of International Standards. The International Organization for Standardization and the International Electrotechnical Commission formed a joint technical committee to establish standards the PIV card complies with. These standards are prefaced by ISO/IEC. Some of these are discussed in the following sections.

1.1 Contactless Chip

The contactless chip complies with ISO/IEC 14443 Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards. There are four parts to this standard: 1) Physical characteristics; 2) Radio frequency power and signal interface; 3) initialization and anti-collision; and Transmission protocols. The contactless chip gets it power from a Proximity Coupling Device (PCD). If you were to look at a contactless only device, it is completely encased in plastic (no metal contacts visible). The second interface is for data transfer. The device operates at a frequency of 13.56 MHz with a data rate of 106K bits per second. Unlike other radio frequency ID approaches, the contactless chip must be in close proximity to the PCD (hence the alias “proximity card”). Starting with PIV part II, the Cardholder Unique Identifier (CHUID) is required to be resident on the contactless chip. In order to satisfy the PIV requirements, the chip need only act as a data store.

In the initial draft version of the FIPS 201 *Personal Identity Verification (PIV) of Federal Employees and Contractors*, a biometric was to be included. However, in the final FIPS, the contactless chip is simply the CHUID holder. Proximity card readers have the ability to read the contents from the chip. To protect the originally envisioned biometric information, FIPS 201, page 8, included the following requirement: *Specifically, employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV credential.* Initially, it was feared was the contents could be read without the user’s knowing the fact. However, it was decided that the biometrics were best protected by the contact chip

which requires a user to enter a personal identification number (PIN) before access to the contact chip is permitted. Consequently, FIPS 201 does not allow biometrics it in the contactless chip.

Even with only the CHUID stored on the contactless chip, this chip is not without risk. Consider that any compliant reader can extract the objects stored on the chip. While an opaque sleeve might offer protection against casual card reading, it cannot protect against the myriad of social engineering attacks. For example, a card holder is asked to show their government ID at some function, store, or as part of some ongoing investigation to a bad actor. The bad actor then removes the badge from its sleeve, places it next to a contactless reader, and captures the CHUID. Later the bad actor could copy the captured CHUID onto a bogus card and gain access to federal facilities based on the legitimate CHUID presented by the bad actor. Moreover, the digital signature on the copied CHUID would also validate as being correct. It is for this reason I believe the contactless chip will migrate to a microprocessor with an embedded cryptographic module that is PIN activated.

1.2 Contact Chip

Like the contactless chip, the contact chip complies with international standards. In this case, ISO/IEC 7816 *Identification Cards—Integrated Circuits with Contacts*. This standard is also divided into parts. If you look at a contact chip smart card, you will see eight metallic pads[1]. These pads are directly wired to the internal microelectronic circuitry (typically a microprocessor). Table 1 explains what the pads are used for.

Chip Pad	Description
I/O	This is the input/output pin. Data is transferred serially through this pad.
VPP	Some devices allow programs to be burnt into memory. To do this, a programmable voltage is applied to this pad
GND	Ground (reference voltage)
CLK	Like standard computers, the contact smart card chip requires and external clock
RST	This pad applies a reset to place the chip in a known starting state.
VCC	The chip requires its power form an external source. This pad is used to support voltage
RFU	There are two pads Reserved for future use.

Table 1 Contact Chip Pad Descriptions

The contact chip also includes a FIPS 140-2 validated cryptographic module. This module includes mathematical functions optimized in silicon. This later capability is necessary for performing the cryptographic functions performed during public key encryption. To activate the contact chip a proper PIN is required. For this reason, the contact chip provides stronger Identification and Authentication (I&A). The contactless chip will be used for lower assurance high volume entrances.

The contact chip can support digital signatures and the secure exchange of encryption keys. Some may ask, well what happens if I leave my badge in the smartcard reader? If a badge is left in the reader, to calculate a digital signature, the card holder must enter in the correct PIN. Consequently, without the PIN, the PIV card cannot generate digital signatures. Currently, the PIN is limited to 8-byes of information. Values

[1] Pads are metal contacts located on the PIV card.

less than 8-bytes are padded with 0xFF (all ones). The final version of SP 800-73 shows an example on page 20 where the PIN is represented by digits (values 0 – 9 inclusive) represented in American Standard Code for Information Interchange (ASCII) format. There does not appear to be any restrictions allowing other characters to be used for the PIN. Consequently, if a user at their keyboard selects an alpha-numeric PIN, then for key pad reader devices that only have values 0 – 9, the user would not be able to properly authenticate. The PIV cards also allow a limited number of attempts before the card locks up. This is a selectable value determined by the issuing agency. At the PIV card, the value is decremented at each failed attempt until the tries left is zero. At that time, the card PIN or try retry counter must be set by a person with administrative rights to the card management system. This is also the scenario when a user forgets his or her password. Currently, the card lockout scenario only pertains to the contact chip. An interesting aspect of the PIN activated contact chip is that for biometrics, is the use of three factor[2] authentication.

1.3 Printed Material

The PIV card includes a set of required and optional printed material. This section focuses only on the mandated printed material. There are five items on the front and two on the back required for PIV compliance. The front matter must include the following:

- Photograph using a minimum resolution of 300 dots per inch,
- Full name,
- Employee affiliation,
- Organizational affiliation, and
- Expiration date.

The back side includes the following:

- Agency card serial number, and
- Issuer identification

Additionally, the card must include some resistance to tampering. Technologies cited include:

- Optical varying structures,
- Optical varying inks,
- Laser etching and engraving,
- Holograms,
- Holographic images, and
- Watermarks.

2 What is in a PIV Card?

The PIV card includes a number of mandated and optional data elements. At a minimum, PIV cards contain a PIN, a CHUID; PIV authentication (certificate and key

[2] There are three factors to authentication an individual: Something you know (such as a PIN or password); something you have (such as a smart card token), and something you are (biometric).

pair); two biometric (fingerprints); a security object (PKI for Machine Readable Travel Documents), and a card capability container. The biometric, authentication certificate, CHUID, and security object each are digitally signed. To comply with the common policy [1], each digital signature requires the signed to enter in their PIN. Thus, there are at least five signatures required to issue a PIV card. These data elements along with the encryption and digital signature key pairs are discussed in this section.

2.1 CHUID

The CHUID data element is kept in both the contact and contactless chips. It includes a 16 byte Global Unique Identifier (GUID), a 25-byte Federal Agency Smart Credential Number (FASC-N) [2], expiration date, authentication key map, and issuer digital signature. The CHUID contains several data elements listed below: he GUID and FASC-N are discussed further in this section.

- FASC-N (25-bytes)
- Agency Code (4-bytes)
- Organization Identifier (4-bytes)
- Data Universal Numbering System (DUNS) (9-bytes)
- GUID (16-bytes)

2.1.1 FASC-N

Prior to the FASC-N, there was another identifier defined by the Security Equipment Integration Working Group (SEIWG-12) [3]. This sting included the person's social Security Number (SSN) in the form of binary coded decimal (BCD) digits[3]. The FASC-N requires 40 characters be encoded. As noted in the last footnote, 5-bits are used to represent each character resulting in a 200-bit (25-byte) FASC-N. The FASC-N is backward compatible with the SEIWG-12 so this could impact an individual's privacy if implemented incorrectly. Whereas the SEIWG-12 required the cardholder's SSN, the FASC-N does not have to include a SSN; and it is strongly recommended that implementers not use the SSN.

Some other fields are agency code, system code, credential number, personal identifier (this is the field that would contain the SEIWG-12 SSN), organizational identifier, individual credentials issued (how many times your credential was reissued), a organizational category, a person/Organization association category, and a credential series. The other fields are separators and error checks. Although the original intent of FIPS 201 was for federal employees and contractors, some of the FASC-N fields identify those outside of government. For example, the Organizational Category (OC) has the following values:

1 - Federal Government Agency

2 - State Government Agency

3 - Commercial Enterprise

4 - Foreign Government

[3] Binary Coded Decimal (BCD) Digits used 4-bits to represent number 0 – 9. A 4-bit number can represent 16 possible values (in binary from 0000 to 1111). The set of possible values is (0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, & 111). However, the FIPS implementation uses an odd parity bit thereby requiring 5-bits per BCD digit.

The full FASC-N has 17 separate fields. These fields are depicted in the order they occur in the following table.

Field	Description
SS	Start Sentinel: Indicates that the start of data is the next character. This is typically used for magnetic strips.
Agency Code	4-characters representing the government agency issuing the credential.
FS	Field Separator (Cannot be used for data)
System Code	4-characters that identify the system the card is enrolled in. The FIPS requires the system code be concatenated with the credential number to create an extended number with 10 billion unique numbers.
FS	Field Separator
Credential Number	6-characters generated by the issuing agency. No duplicates are allowed.
FS	Field separator
CS	Credential Series that reflects major system changes
FS	Field Separator
ICI	Individual Credential Issue is incremented each time a card is lost or replaced.
FS	Field Separator
PI	Personal Identifier to uniquely identify the card holder.
FS	Field Separator
OC	Organizational Category
OI	4-charaters representing the Organizational Identifier
POA	Person/Organization Association
ES	End Sentinel: This follows the last character of data. This is typically a required field when using a magnetic strip.
LRC	Longitudinal Redundancy Character, a bit error detection value

Table 2 – Federal Agency Smart Credential Number Format

Of interest is that when the Agency Code is 9999, it represents a non-federal entity. In these cases, the DUNS value located in the CHUID is used will represent the credential issuer. That is, the mechanisms necessary for non-government use were considered up front. As a final point, the authentication certificates could include privacy information. As noted in FIPS 201, section 5.4.5.1 and copied below:

> PIV Authentication certificates contain the FASC-N in the subject alternative name extension; hence, these certificates shall not be distributed publicly via LDAP or HTTP.

This will require SSPs to restrict distribution of authentication certificates.

2.1.2 GUID

The SP 800-73 requires the following:

> The GUID shall be present. If assigned, the GUID should be encoded as IPv6 address. Otherwise, its value should be 0x00.

One of the items necessary is to have a way to uniquely identify each individual and card. It is hopped that the 128-bit IPv6 address will serve this purpose. Currently, most IP implementations are based on IPv4 with a 32-bit address. That the GUID is mandatory might be an indicator where the standards people plan to focus their attention during the coming years.

2.2 Biometrics

The contact chip will hold two digitally signed biometrics data elements. These will correspond to the left and right index fingers. The National Institute of Standards and Technology (NIST) Special Publication 800-73 has a formula for selecting other fingers as needed. The fingerprints are in the form of a scanned image 368 by 425 pixels. Due to space limitation on the PIV cards, cropping to no less than 320 by 320 pixels is permitted and a compression algorithm is allowed [4] as modified by [5]. For fingerprint scanners; the Federal Bureau of Investigation (FBI) requires a resolution of at least 500 pixels per inch with an error of plus or minus 5 pixels per inch [6]. However, at this time, it would seem that the fingerprint will be stored as an image. On a separate matter, the actual fingerprint recognition algorithms are typically minutiae and correlation based. Each algorithm has its strengths and weaknesses. However, it has been suggested that the minutiae format would require less storage space on the contact chip. Nevertheless, at this time, the format stored is a scanned image (possibly chopped and compressed).

The biometrics follow the Common Biometric Exchange Format Framework (CBEFF) as defined in FIPS 201. The CBEFF includes the FSAC-N and uses the integrity option (digitally signed). For FIPS 201 compliance, the confidentiality option (encryption) is not used.

2.3 Key Pairs

There is one mandatory key pair (Authentication) and three optional Key Management, Digital signature, and Card Authentication. The card authentication (and possible another key for card management) could also be supported as symmetric[4] keys. When using asymmetric keys (public key encryption), the public key is contained within the X.509 certificate while the private key is maintained within the smartcard. This section will describe three of the key pairs used and methods for revocation.

2.3.1 PIV Authentication

This is the only mandatory key pair required by FIPS 201. The certificate includes the FASC-N within the subject alternate name. That is, the certificate contains the same FASC-N as is found in the CHUID. Indeed, one of the authentication methods checks

[4] Symmetric keys use the same key for encryption and decryption. In contrast, the asymmetric key for encryption is different from that used in decryption.

the FASC-N numbers from each signed object to verify consistency. The PIV cards will typically include the id-fpki-common-hardware certificate policy extension.

Recall that the FASC-N is backward compatible with the SEIWG-12. Thus, depending on how the FASC-N is defined, it could include a user's SSN. As a result, the Authentication certificates cannot be widely distributed due to the potential of information in identifiable format (IIF). Perhaps the easiest way around this issue is to establish a policy that the SSN will not be used within the FASC-N.

2.3.2 Digital Signature

Although the digital signature key pair is listed as optional, for those involved with the certificate issuance, they will certainly need a digital signature key pair. The digital signature key pair supports non-repudiation. Thus, every time there is a digital signature, the cardholder must enter in his or her PIN. Another feature is that the private signature key never leaves the PIV card. In order to digitally sign an object, the PIV card must be used. This provides a powerful control that works with a number of applications such as Secure Multipurpose Internet Mail Extensions (S/MIME) email.

2.3.3 Key Management

Another optional key pair supported is for key management, or encryption. These keys are used to securely exchange symmetric encryption keys. Encryption offers some unique challenges when applied to archived documents. That is, if the encryption key is not available, the encrypted document can never be used in a meaningful manner[5]. The typical approach to maintaining key history is to have some centralized key repository. Thus, if an individual loses their PIV card they can get a copy of the key management key and thereby decrypt any of their encrypted documents. Of course, the key repository is equivalent to a platform with the keys to the kingdom and typically requires extensive protection mechanisms. It in effect becomes one of the most sensitive machines within an organization.

2.3.4 Verifying Keys are Valid

One of the key features of PIV cards is the ability to check if the key pairs are still valid. To accomplish this, FIPS 201 requires two verification mechanisms; a revocation list and an Online Certificate Status Protocol (OCSP) responder. The revocation list is accessed using either the Lightweight Directory Access Protocol (LDAP) or by Hypertext Transport Protocol (HTTP). The public key is kept in an X.509 certificate that includes a CRL Distribution Point (CDP). The CDP also specifies the protocol used to get the CRL. In this manner, applications have all the information needed to automatically retrieve the revocation list and validate that the certificate is still valid. Likewise, certificates supporting OCSP will include the AuthorityInfoAccess extension.

OCSP [7] is a protocol that applications can use to check the status of certificates. There are three digitally signed OCSP responses, good, revoked, or unknown. The reason OCSP was developed was that as CRLs become large, the time to pull them down from the CDP and then check to see if a certificate (or a path certificate) is valid grows accordingly. With OCSP, the responder can be optimized to do

[5] Encryption takes meaningful text and converts it to cipher text (gibberish). The process of decryption converts the cipher text back into the original meaningful text. This is only possible with the correct symmetric key.

the checking and the information exchanged is reduced. Therefore, for some larger environments with large revocation lists, OCSP can offer speed improvements.

2.4 Security Object

The security object complies with Technical Report "PKI for Machine Readable Travel Documents (MRTD) offering ICC read-only access" in accordance with International Civil Aviation Organization (ICAO) 9303 for MRTD. This is a mandatory object located in the contact chip. The ICAO document describes a country signing Certification Authority (CA) which could add some complexity to the PIV card authentication mechanism. However, there are some differences between the PIV certificate and the ICAO. In the ICAO, the extension for certificate policy is optional, the Subject Alternate Name is not to be used, and Name Constraints not used. While there may be some compatibility issues with the certificates, it is interesting to note that one possible use of the security object is with passports. The certificate associated with the object signing key must include the ICAO Public Key Directory within the KDP. It should be noted that the KDP can include multiple entries.

3 How the Cards Authenticate

The PIV cards can be used to authenticate cardholders based on the printed information, with the contactless, and that within the contact chip. This section describes several methods for authenticating cardholders. SP 800-73 describes the following three validation steps:

- Card Validation: The process of verifying that a PIV Card is authentic (i.e., not a counterfeit card) and has not been subjected to tampering or alteration.
- Credential Validation: The process of verifying the various types of credentials (such as visual credentials, CHUID, biometrics, PIV keys and certificates) held by the PIV Card.
- Cardholder Validation: The process of establishing that the PIV Card is in the possession of the individual who is the legitimate owner of the card.

Those authentication methods requiring the contact chip are presented in this section. NIST SP 800-73 lists a PIV application, API, Local System, and the PIV Card Edge. In the first figure, the authentication is done by getting the CHUID from the PIV card and having the PIV application verify the expiration date and signature associated with the CHUID. If these are okay, then the cardholder is authenticated. Otherwise, the authentication request is rejected. It should be noted that in this scenario, the cardholder does not enter a PIN. Additionally, there is no local system processing required.

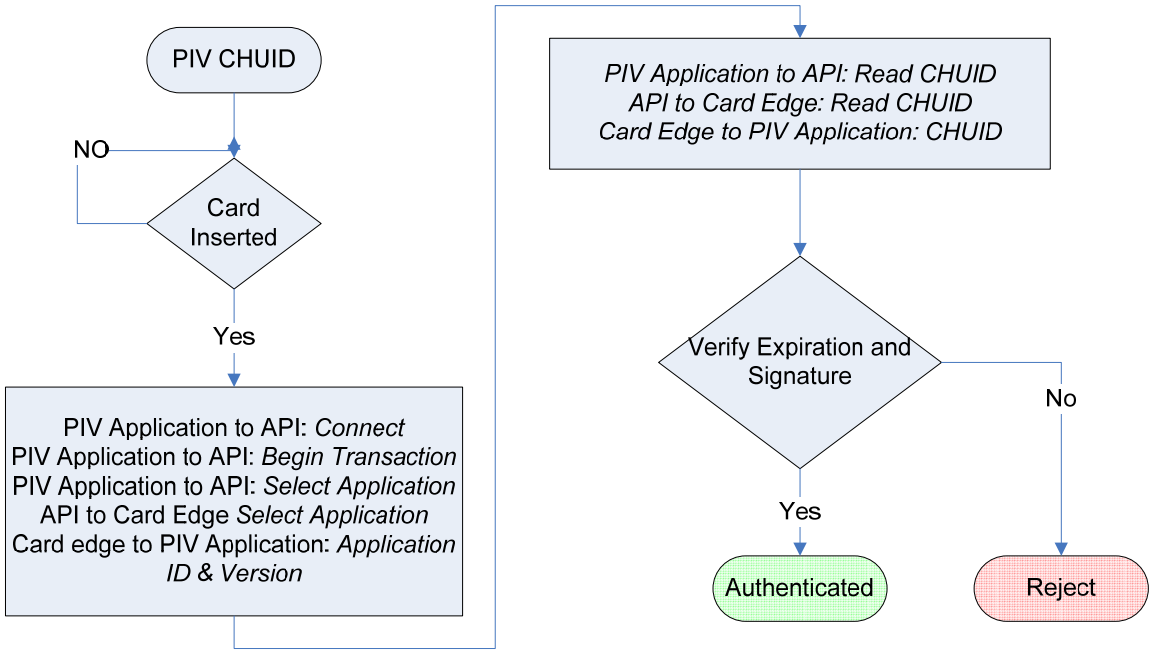

Figure 1 CHUID Authentication

The next example uses the same CHUID retrieval and authentication. To reduce the redundancy, the next flowchart (Figure 2) will use a single decision to represent the Figure 1 flowchart. Figure 2 depicts biometric authentication. Note, acquire biometric process can either be attended or unattended. This could be accomplished by using a biometric reader connected to a local computer. In the case of attended, there is someone watching to verify that the biometric is taken form the card holder. The biometric readers could be part of a facility access system or as part of a computer. In the case of the facility, the readers would likely be located in front of doors that would open once the biometric is verified. This would likely be an example of an unattended biometric. There could also be biometrics located at a front entrance where security guards are located. This would be an example of an attended biometric. Finally, there could be biometric readers located at computers. These would also be examples of unattended biometrics. However, given that the computer would require a smartcard reader to get the biometric and that the PIV card must include an authentication key pair, there appears to be no advantage in deploying biometric readers on client workstations. The exception would be in cases where both the PKI and biometric authentication are verified. In the case of capturing the biometric, SP 800-73 depicts each use case diagrams separately. However, the focus of this section is to examine the transactions.

Unlike the CHUID, the cardholder PIN must be validated before the biometric is allowed to be read from the PIV card. Thus, even if the card is lost, a bad actor could not extract the biometric information without knowing the proper PIN. Note the FASC-N located within the biometric is checked. As noted in FIPS 201 “The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.”

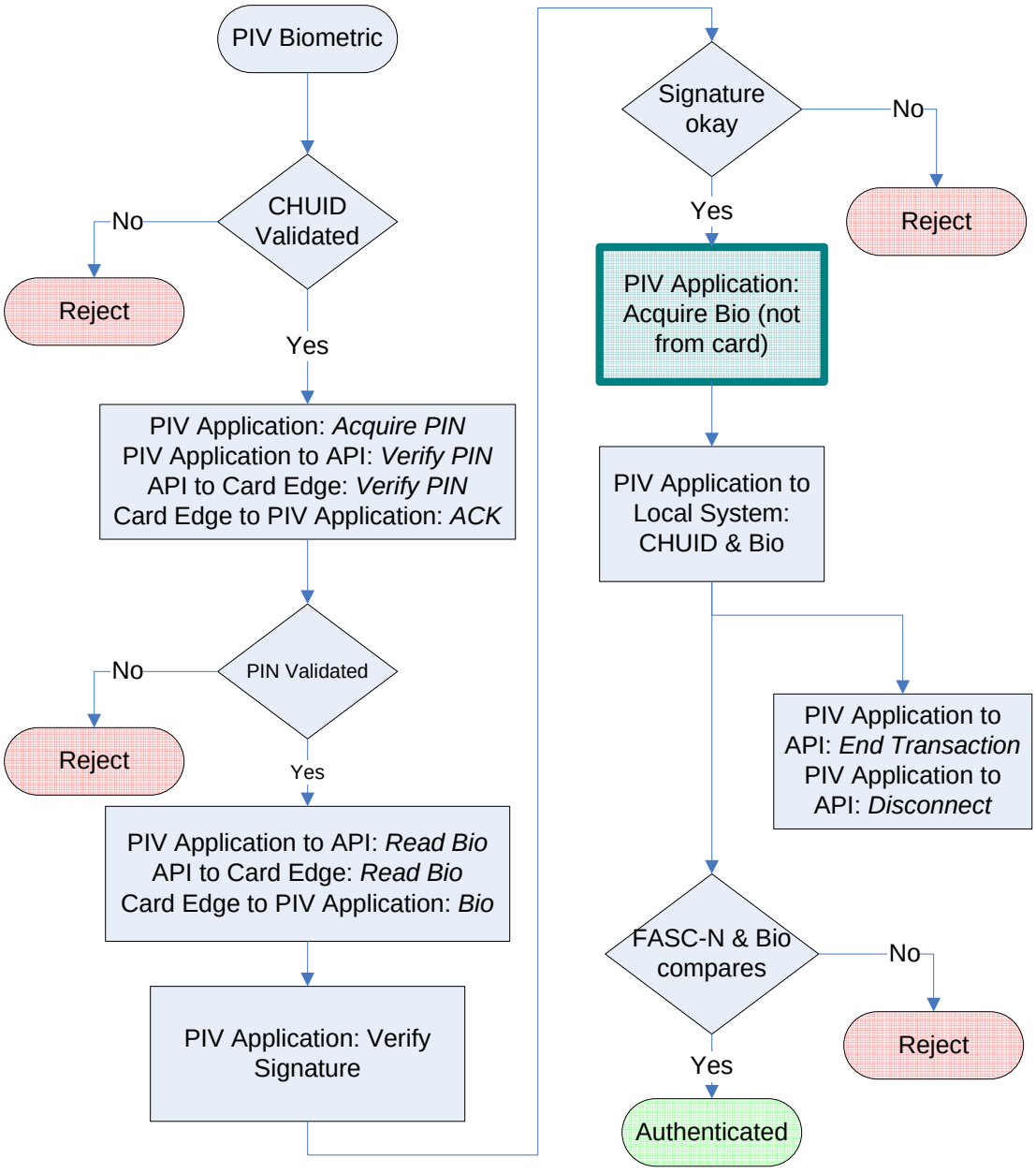

Figure 2 Biometric Authentication

The next figure illustrates how the PIV authentication key is used to authenticate the cardholder. Note the PIV authentication certificate moves off of the PIV card before the PIN is entered. Next, the cardholder is digitally signing a nonce (random string). The digital signature can be verified thereby showing that the cardholder has a valid credential, knows the PIN, and has the PIV card containing the proper PIV authentication key pair. The authentication certificate contains the FASC-N in the subject alternate name extension. This is compared to the FASC-N located in the CHUID.

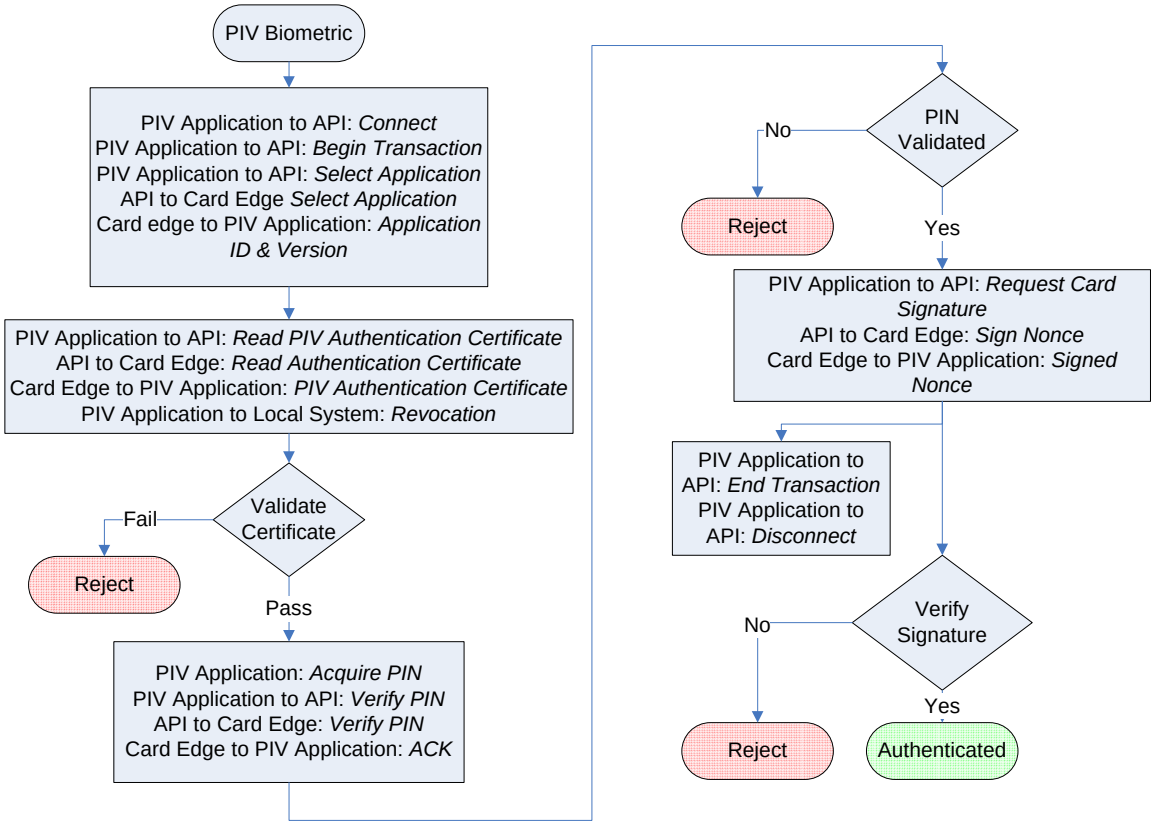

Figure 3 PKI Authentication

In this section, three authentication methods were discussed. PIV cards will be used to authenticate for access to facilities and logical access to computers and networks. FIPS 201 has defined levels of assurance based on the different authentication means. As noted in Table 3, there are four authentication schemes compared with the degree of confidence resulting form each. The BIO is short for unattended biometric and BIO-A corresponds to attended biometric. In this table, the attended biometric has the same assurance provided by the PKI.

This description taken from SP 800-63 differs from FIPS 201. In the FIPS 201 description, the first action is that the cardholder is prompted for their PIN. "The submitted PIN is used to activate the card." This implies that the certificate cannot be extracted before the PIN is entered. At this time, it is unclear which NIST document is correct. Nevertheless, if the FASC-N does not include an SSN, then reading the authentication certificate from the PIV card would not be problematic.

The use cases did not include the other (optional) key pairs located on the PIV card. The main reason is these keys would support various applications and not necessarily be used for authentication purposes. However, there are some online protocols that send a random challenge and have the user digitally sign the challenge. These scenarios are outside the scope of the FIPS 201 document. In the case of the digital signature key, it requires the cardholder enter the correct PIN for each signature. In contrast, the encryption key could be used to for multiple encryption operations with a single PIN activation.

	CHUID	BIO	BIO-A	PKI
Some Confidence	X	X	X	X
High Confidence		X	X	X
Very High Confidence			X	X

Table 3 Logical Authentication Assurance Levels

The next table 4 illustrates authentication applied to facilities. Note that a visual inspection is included in this table. Again, the BIO-A and PKI offer the highest level of assurance.

	Visual	CHUID	BIO	BIO-A	PKI
Some Confidence	X	X	X	X	X
High Confidence			X	X	X
Very High Confidence				X	X

Table 4 Facilities Authentication Assurance Levels

4 When to Convert an Application

In this last section, we described the various types of authentication provided by the PIV card. To facilitate the discussion, we use the OMB and NIST notation applied to the e-Authentication initiative. The OMB provided guidance for Electronic Authentication [8]. The OMB specifically describes the following process that is to be used by Executive branch agencies and departments:

1. Conduct a risk assessment of the e-government system.

2. Map identified risks to the applicable assurance level.
3. Select technology based on e-authentication technical guidance.
4. Validate that the implemented system has achieved the required assurance level.
5. Periodically reassess the system to determine technology refresh requirements.

In the OMB memorandum, applications are assigned four assurance levels. These levels are states in Table 5. The OMB also provides federal agencies with a risk assessment tool to help identify what assurance level applications reside at. The tool is called the "e-Authentication Risks and Requirements Assessment Tool," or e-RA. It was developed by the Carnegie Mellon University (CMU) under funding by the General Services Administration (GSA). The tool uses a Microsoft Access database and is supported by an activity guide [9]. The e-RA focuses on business transactions and the authentication required for each. The people performing the analysis go through each application transaction. The tool allows risk based decisions such that authentication levels can be lowered if costs or other drivers dictate. Well inputted data should provide a reasonable assessment.

Assurance Level	Description of when to use
Level 1	Little or no confidence in the asserted identity's validity
Level 2	Some confidence in the asserted identity's validity
Level 3	High confidence in the asserted identity's validity
Level 4	Very high confidence in the asserted identity's validity

Table 5 OMB M-04-04 Assurance Levels

If there are any risk adjustments, such as increased risk tolerance, it is best to document the justification in the e-RA process. The OMB memorandum [8] requires that potential harm (or impact) and likelihood of occurrence be documented. Further, six categories of harm are specifically identified:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations.

To support the OMB memorandum, the NIST prepared Special Pub 800-63 that defines the type of tokens necessary to support the four assurance levels. Table 6 lists the various types of tokens and identifies what level of authentication they provide. As noted in the NIST recommendation, passwords are considered appropriate only for assurance levels 1 and 2. Assurance levels 3 and 4 require stronger authentication than is provided by a password. The e-RA tool focuses on one application at a time. In actuality, there may be many applications that fall into a given category. A common authentication control could be amortized across multiple applications capable of using the technology. That is, while the cost to implement a change to one application might

be too great, if the same control can be applied to many applications, then the cost per application might be acceptable. For example, a common forms package that can utilize cryptographic certificates might be too costly to justify for one application. However, if the forms are easily incorporated into a number of applications, then the business case is easier to make. Large federal applications typically use Exhibit 300s to describe controls. These in turn are rolled up into an Exhibit 53. It is at the Exhibit 53 level where commonality across applications should be evident. If an application is determined to be a level 3 or 4, and the primary users have PIV cards; then it is a good candidate to convert to PIV card usage instead of deploying yet another technology at a lower assurance level.

Token	Description of when to use
Password tokens	can satisfy the assurance requirements for Levels 1 and 2
Soft cryptographic tokens	may be used at authentication assurance Levels 1 to 3, but must be combined with a password or biometric to achieve Level 3
One-time password devices	are considered to satisfy the assurance requirements for Levels 1 through 3, and must be used with a password or biometric to achieve Level 3
Hard tokens that are activated by a password or biometric	can satisfy assurance requirements for Levels 1 through 4

Table 6 Token Assurance Levels

Summary

In this paper, we discussed the PIV card technology and mandatory content. An examination of the various key pairs and authentication use cases was presented. Finally, there was comparison between the PIV card and e-Authentication. Not covered in this paper were the registration processes required in the PIV card issuance. Likewise, the other possible uses for PIV cards were omitted. The PIV card is a powerful security control that promises to provide strong identification and authentication (I&A). For without I&A, there is little basis for much of security.

References

1. X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, http://www.cio.gov/ficc/documents/CommonPolicy.pdf.
2. Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Government Smart Card Interagency Advisory Board, Version 2.2, July 30, 2004.
3. NIST Interagency Report 6887 - 2003 Edition, Government Smart Card Interoperability Specification Version 2.1, July 16, 2003.
4. International Committee for Information Technology Standards, Elements of Conformance Testing Methodology for Finger Image Based Data Interchange Format of ANSI INCITS 381-2004.
5. NIST Draft Special Publication 800-76.
6. Criminal Justice Information Services (CJIS), *Electronic Fingerprint Transmission Specification*, CJIS-RS-0010 (V7), Section 2.0, Page 101, January 29, 1999.
7. Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, Network Working Group, June 1999.

8. The Office of Management and Budget, Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003.
9 Carnegie Mellon, e-Authentication Risk and Requirements Assessment e-RA Tool Activity Guide For use with e-RA Tool version 1.4b, May, 2004, located at: http://www.cio.gov/eauthentication/documents/eraguide.pdf.