ICAM

Identity, Credential,
& Access Management

CIO
COUNCIL

Federal Identity, Credentialing, and Access Management

Personal Identity Verification Interoperable (PIV-I)
Frequently Asked Questions (FAQ)

Version 1.0

June 28, 2010

Table of Contents

1. Introduction

1.1 Background

Non-Federal Issuers (NFIs) of identity cards have expressed a desire to produce identity cards that can technically interoperate with Federal government Personal Identity Verification (PIV) systems and can be trusted by Federal government Relying Parties. In response to this, the Federal government's Federal CIO Council released the *Personal Identity Verification Interoperability for Non-Federal Issuers* guidance in May 2009, which provides information for entities wishing to implement an identity card that is technically interoperable with a Federally-issued PIV card and can be trusted by Federal relying parties. Subsequently, a revised X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) has been published that comprehensively addresses PIV-I.

1.2 Objective

The objective of this document is to answer the most frequently asked questions regarding what a PIV Interoperable (PIV-I) NFI card is and the interoperability of PIV-I NFI identity cards with PIV systems.

This document is not intended to conflict with existing Federal directives, policies and standards, and where there is a conflict, the authoritative documents listed in Section 3, References, can be relied upon.

2. Frequently Asked Questions

2.1 What is a PIV-I Card?

A PIV-I (Personal Identity Verification – Interoperable) Card meets the PIV technical specifications to work with Federal PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal government Relying Parties to trust the card. The PIV-I Card is suitable for level of assurance 4 as defined in OMB Memorandum M-04-04 and NIST SP 800-63, as well as multi-factor authentication as defined in NIST SP 800-116.

The following is a brief summary of the PIV-I guidance, which identifies the areas in which NFIs cannot meet the full PIV standard as specified by FIPS 201, and provides alternatives. There are four core areas identified:

Core Area	Description
Credential numbering	FIPS 201 defines the use of the FASC-N. This credential numbering schema cannot be used by non-Federal issuers. X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) provides the solution using an RFC 4122-conformant UUID. The UUID is found in the certificates, signed objects, and the GUID TLV of the CHUID.
PKI technology mapping	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework defines an object identifier (OID) that is specific to Federal issuers. Non-Federal issuers must map their policies to the PIV-I Hardware policy OID and be cross-certified with the FBCA to meet the requirements of PIV-I. See FAQ 2.3 for an overview

Core Area	Description
	of the PIV-I Hardware OID.
Background investigation	FIPS 201 defines the use of a National Agency Check with Written Inquiries (NAC-I) for PIV. The NAC-I is only available to Federal agencies through the Office of Personnel Management. X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) specifies the PIV-I Hardware policy as the identity verification model that separates identity verification from the NAC-I suitability and fitness adjudications. See FAQ 2.3 for an overview of the PIV-I Hardware policy[1].
Visual Distinction	The PIV-I Card physical topography shall include, at a minimum, the following items on the front of the card: cardholder facial image; cardholder full name; Organizational Affiliation, if it exists, otherwise the issuer of the card; and card expiration date. However, visual distinction of a PIV-I Card from that of a Federal PIV Card is required to ensure no suggestion of attempting to create a fraudulent Federal PIV Card.

2.2 What is the difference between a PIV-I Card and a PIV Card?

The term "PIV Card" may only be used to describe an identity card that is fully conformant with Federal PIV standards (i.e., FIPS 201 and related documentation). Only a Federal entity is capable of fully meeting these standards and issuing a PIV Card. A PIV-I Card meets the PIV technical specifications of NIST SP 800-73 and is issued in a manner that may be trusted by Federal Government Relying Parties, but does not meet all of the requirements of FIPS 201.

In addition, the following table highlights the differences and similarities between a PIV Card and a PIV-I Card in the areas of suitability, trust, and card edge.

[1] PIV-I Hardware requirements are consistent with NIST SP 800-63.

		PIV Card	PIV-I Card
Identity Verification	NIST SP 800-63, Assurance Level 4	●	●
	NACI	●	
Trust	FIPS 201 Conformant	●	
	PIV OID on PIV Authentication Certificate (trust model)	●	
	PIV-I Hardware equivalent Authentication Certificate[2]	●	●
	PIV-I Content Signing equivalent object signing certificate	●	●
Card Edge	Card Stock on GSA APL[3]	●	●
	PIV Application Identifier (AID)	●	●
	Command edge and NIST SP 800-85 conformant[4]	●	●
	NIST SP 800-73 conformant GUID present in the CHUID	●	●
	RFC 4122 conformant UUID required in the GUID data element of the CHUID[5]		●
	RFC 4122 conformant UUID present in the Authentication Certificates[6]		●
	Visually distinguishable from PIV Card		●

[2] Certificate equivalence for NFIs is established by the FBCA. See FAQ 2.3 for an overview of FBCA PIV-I policies.

[3] Conformant form factor.

[4] Contact and contactless command edge conformant defined in NIST SP 800-73 Part 2 requires support for specific ISO/IEC 7816 commands. Card edge and data model verified through NIST SP 800-85B tool (further efforts are expected to address exceptions for NFIs). Card edge specifications verified through the NIST Personal Identity Verification Program (NPIVP).

[5] NIST SP 800-73 does not require the use of RFC 4122 in the generation of a valid GUID for PIV cards, but it is required for NFI PIV-I cards.

[6] The value of the UUID will be in the subjectAltName extension of the PIV Authentication Certificate and the Card Authentication Certificate.

2.3 What OIDs are specified for PIV-I?

The following table specifies the OIDs defined specifically for PIV-I:

Name	Type	Purpose	Status	Value
id-fpki-certpcy-pivi-hardware	Policy OID	Conveys certificate policy compliance in certificates whose keys require activation by the PIV-I Cardholder (e.g., PIV-I Authentication, PIV-I Digital Signature, and PIV-I Key Management keys).	Defined	2.16.840.1.101.3.2.1.3.18
id-fpki-certpcy-pivi-cardAuth	Policy OID	Conveys certificate policy compliance in certificates whose keys do not require PIV-I Cardholder activation (i.e., PIV-I Card Authentication key)	Defined	2.16.840.1.101.3.2.1.3.19
id-fpki-certpcy-pivi-contentSigning	Policy OID	Conveys use by a Card Management System that complies with the certificate policy.	Defined	2.16.840.1.101.3.2.1.3.20
id-fpki-pivi-content-signing	EKU OID	Conveys that the key is intended to be used to sign PIV-I Cards	Defined	2.16.840.1.101.3.8.7

There is no Card Authentication extended key usage (EKU) OID defined specifically for PIV-I. PIV-I Card Authentication certificates must assert the PIV Card Authentication EKU OID (id-PIV-cardAuth) in the EKU extension to specify that the public key is used to authenticate the PIV-I card rather than the PIV-I cardholder.

2.4 Can my agency accept PIV-I Cards issued by our contractors' company in lieu of issuing PIV Cards to these individuals?

No. Individuals who fall within the applicability of HSPD-12 (see OMB M-05-24 for details), including Federal contractors requiring routine access to Federally-controlled facilities or Federally-controlled information systems for a period of time greater than 6 months, must continue to be issued PIV Cards by the Federal Government in accordance with relevant policies.

2.5 Can non-PIV Cards issued by the Federal Government be considered PIV-I?

Yes. The Federal Government may issue non-PIV identity and access cards to individuals who are outside the applicability of HSPD-12. Federal Government PIV Card Issuers may issue non-PIV identity cards that meet the PIV-I requirements specified in the X.509 Certificate Policy for the FBCA. The X.509 Certificate Policy for the FBCA specifies the minimum requirements for the Federal Government to rely on PIV-I NFI identity cards. Example scenarios where this might apply include facility access cards issued to short term employees (e.g., summer interns) and identity credentials issued by the Legislative and Judicial Branches of the Federal Government.

2.6 Can a PIV-I Card be accepted for both physical and logical access?

Yes. A PIV-I Card may be used to access both physical and logical resources. However, each Federal Government Relying Party will determine the extent to which it will trust PIV-I Cards to access resources within its areas of control.

2.7 Can an identity card issued by a program that has modified the PIV technical specifications be considered a PIV-I Card?

No. In order to be considered PIV-I, an identity card must conform to the minimum PIV technical requirements defined in X.509 Certificate Policy for the FBCA, and be issued by an issuer who has been assessed by the Federal PKI Policy Authority as meeting those requirements.

2.8 What is the PIV-I Card Logical Data Model?

The PIV-I Card logical data model is the same model as the PIV Card logical data model, as defined in FIPS 201 Section 4.1.5.1 and further detailed in NIST SP 800-73 Part 1. To support a variety of authentication mechanisms, PIV-I Card logical credentials shall contain multiple data objects for the purpose of verifying the cardholder's identity at graduated assurance levels. Some of the data objects that are optional for PIV have been made mandatory for PIV-I. See FAQ 2.11 for the list of mandatory PIV-I data objects.

2.9 Can the PIV-I Card Logical Data Model be extended?

Yes. The PIV-I Card logical data model can be extended in the same way as the PIV Card logical data model, as defined in FIPS 201 Section 4.1.5.1. The PIV-I Card logical data model may be extended using the optional data defined within NIST SP 800-73 Part 1.

2.10 What certificates and keys may be present on a PIV-I Card?

Except for the Card Authentication certificate/key pair, PIV-I has the same certificate and key configuration as a PIV Card, as defined in FIPS 201 Section 4.3. The PIV-I Card has two mandatory certificate/key pairs, and three optional certificate/key pairs:

Certificate/Key	Mandatory or Optional	Description
Authentication Certificate/Key	Mandatory	Shall be an asymmetric private key supporting user authentication for an interoperable environment, and it is mandatory for each PIV-I Card. In addition, the Authentication Key is available only on the contact interface and requires the user to present its PIN to the card.
Card Authentication Certificate/Key	Mandatory	Shall contain an asymmetric[7] X.509 Certificate for Card Authentication that conforms to the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards; conforms to NIST SP 800-73; and is issued under the PIV-I Card Authentication policy.

[7] PIV allows either a symmetric (secret) key or an asymmetric key, but NIST SP 800-116 “strongly recommends that agencies use the asymmetric CAK protocol.

Certificate/Key	Mandatory or Optional	Description
Digital Signature Certificate/Key	Optional	Asymmetric private key supporting document signing.
Key Management Certificate/Key	Optional	Asymmetric private key supporting key establishment and transport. This can also be used as an encryption key.
Card Management Key	Optional	Symmetric key used for card personalization and post-issuance activities.

2.11 What are the mandatory data model elements for a PIV-I Card?

The PIV-I Card logical data model is the same model as the PIV Card logical data model, as defined in FIPS 201 Section 4.1.5.1. NIST SP 800-73 Part 1 provides the technical guidance for these required elements. To support a variety of authentication mechanisms, PIV-I Card logical credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels. These mandatory data elements collectively comprise the data model for logical credentials, and include the following:

- A Card Capability Container
- A Cardholder Unique Identifier (CHUID)
- An authentication key (one asymmetric key pair and corresponding certificate)
- A card authentication key (one asymmetric key pair and corresponding certificate)
- Two biometric fingerprints.
- Facial Image Buffer
- Security Object

2.12 What are the optional data model elements for a PIV-I Card?

The PIV Card logical data model defines several optional elements. The PIV-I Card logical data model can be extended in the same way as the PIV Card logical data model, as defined in FIPS 201 Section 4.1.5.1. NIST SP 800-73 Part 1 provides the technical guidance for these optional elements. These options may be selected to meet organization-specific requirements. The optional elements include:

- Printed Information Buffer
- Discovery Object
- Key History Object
- Retired Key Management Keys
- Digital Signature Key
- Key Management Key
- Symmetric key associated with the card management system.

NIST SP 800-78 specifies additional cryptographic algorithms and key sizes and NIST SP 800-76 provides additional biometric requirements.

2.13 What is the validity period for PIV-I certificates?

The validity period of PIV-I certificates is the same as for PIV certificates. For example, the maximum validity of PIV-I certificates is three (3) years, which is also the validity period for human subscriber certificates issued in accordance with FBCA certificate policies. See FAQ 2.3 for an overview of PIV-I in the FBCA Certificate Policy.

2.14 What algorithms must be used in PIV-I Card certificates?

The PIV-I Card must use the same algorithms as the PIV Card for their respective certificates, as specified in NIST SP 800-78. NIST SP 800-78 Tables 3.1 and 5.1 specify the algorithms and key sizes that must be supported per key type:

PIV Key Type	Time Period for Use	Algorithms and Key Sizes
PIV-I Authentication key	Through 12/31/2013	RSA (1024 or 2048 bits) ECDSA (Curve P-256)
	After 12/31/2013	RSA (2048 bits) ECDSA (Curve P-256)
Card Authentication key	Through 12/31/2010	2TDEA 3TDEA AES-128, AES-192, or AES-256 RSA (1024 or 2048 bits) ECDSA (Curve P-256)
	1/1/2011 through 12/31/2013	3TDEA AES-128, AES-192, or AES-256 RSA (1024 or 2048 bits) ECDSA (Curve P-256)
	After 12/31/2013	3TDEA AES-128, AES-192, or AES-256 RSA (2048 bits) ECDSA (Curve P-256)
Digital Signature key	After 12/31/2008	RSA (2048 bits) ECDSA (Curves P-256 or P-384)
Key Management key	After 12/31/2008	RSA key transport (2048 bits); ECDH (Curves P-256 or P-384)
Card Management Key	Through 12/31/2010	2TDEA 3TDEA AES-128, AES-192, or AES-256
	After 12/31/2010	3TDEA AES-128, AES-192, or AES-256

2.15 What is the status of the PIV-I Certificate Policy and PIV-I Profile?

A revised X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) that comprehensively addresses PIV-I has been published. PIV-I policies have been added to all applicable sections, and a new PIV-I appendix has been added for requirements that do not fit into any existing Certificate Policy section. See FAQ 2.3 for an overview of PIV-I in the FBCA Certificate Policy. Also published is a wholly new X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards. The document is based on the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program.

2.16 What must PIV-I Card Authentication certificate policies map to?

The certificate policies for the PIV-I Card Authentication certificate must map to the FBCA's id-fpki-certpcy-pivi-cardAuth policy (see FAQ 2.3 for an overview of the PIV-I card authentication certificate policy). This is done by cross-certifying the issuing CA with the FBCA. Note that a revised X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) that comprehensively addresses PIV-I has been published (See FAQ 2.15).

2.17 What key usage bits must be asserted in the keyUsage exensions of PIV-I certificates?

The certificates on PIV-I Cards assert the same bits in the certificate key usage extension as the respective certificates on PIV Cards[8], as follows:

PIV-I Certificate	Key Usage bits
PIV-I Authentication Certificate	Only digitalSignature shall be set.
PIV-I Digital Signature Certificate	Both digitalSignature and nonRepudiation shall be set.
PIV-I Card Authentication Certificate	Only digitalSignature shall be set.
PIV-I Key Management Certificate	keyEncipherment asserted when public key is RSA. keyAgreement asserted when public key is elliptic curve.
PIV-I Content Signing Certificate	digitalSignature

2.18 Do PIV-I Cards need to be FIPS-140-2 validated?

Yes. the X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) requires FIPS 140-2 validation of PIV-I Cards. In addition, PIV-I Cards must be on the Approved Products List. For more information, see the Acquisition section on idmanagement.gov as well as the FIPS 201 Approved Products List.

[8] See X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program for information on use of the extended key usage extension in certificates on PIV Cards.

2.19 What assurance requirements must PIV-I card issuers meet?

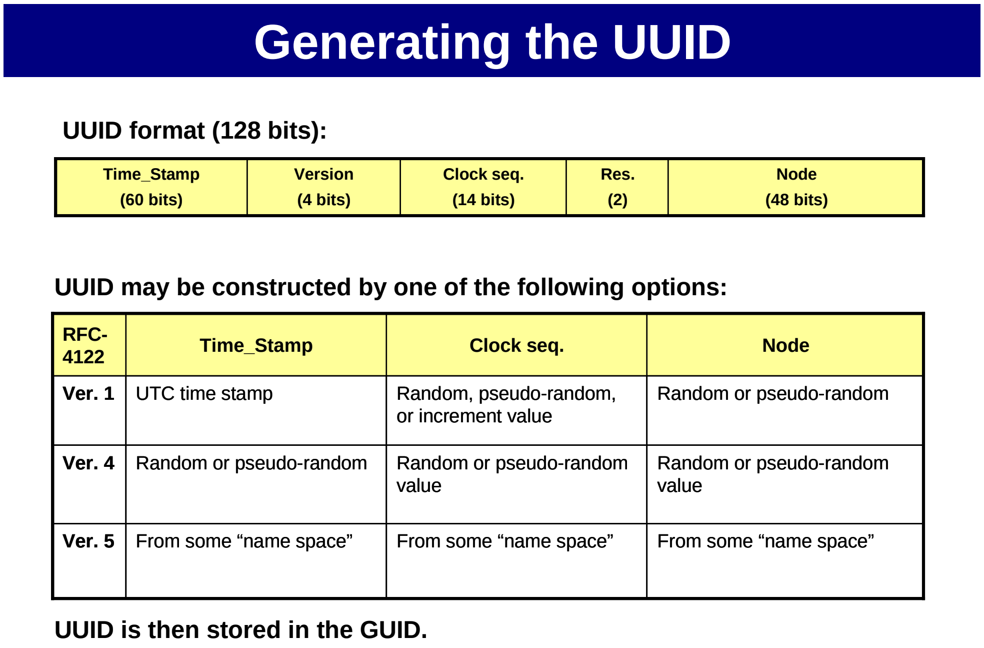
Relying parties can be assured, with a high level of confidence, that PIV-I NFIs are following sound security practices, because:

- Cross Certification with the FBCA includes extensive requirements related to Facility, Management, and Operational Controls (FBCA Section 5) and Technical Controls (FBCA Section 6)
- PIV-I NFIs must cross-certify with the FBCA, which requires a rigorous process of evaluating a PIV-I NFI's policies and procedures against the requirements defined in the X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA);
- PIV-I NFI's will be issued a cross-certificate from the FBCA that will map the NFI's policy OIDs to the relevant PIV-I OIDs (See FAQ 2.3 for more information); and
- Cross-certification with the FBCA requires annual compliance audits to demonstrate ongoing compliance with certificate policies and procedures.

NFI cross certification with the FBCA is a requirement for identity cards to be considered PIV-I.

2.20 What are the valid methods to generate/construct a UUID number?

The following table summarizes the three methods of generating/constructing UUID numbers specified in NIST SP 800-73.



Generating the UUID

UUID format (128 bits):

Time_Stamp (60 bits)	Version (4 bits)	Clock seq. (14 bits)	Res. (2)	Node (48 bits)

UUID may be constructed by one of the following options:

RFC-4122	Time_Stamp	Clock seq.	Node
Ver. 1	UTC time stamp	Random, pseudo-random, or increment value	Random or pseudo-random
Ver. 4	Random or pseudo-random	Random or pseudo-random value	Random or pseudo-random value
Ver. 5	From some "name space"	From some "name space"	From some "name space"

UUID is then stored in the GUID.

There is a slight chance of UUID collision across issuers. Therefore, Relying Parties should check for collisions when new UUIDs are enrolled in a local Physical Access Control System (PACS).

2.21 How does PIV-I handle Global Unique Identification Number (GUID) during issuance?

The GUID is a field that must be in the Cardholder Unique Identifier (CHUID). The value of the GUID must be an RFC 4122 UUID, as specified in the X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA). The UUID value in the GUID is also used in certificates and signed objects on the card.

2.22 What software and hardware can be used to issue PIV-I Cards?

Software and hardware listed on the FIPS 201 Approved Products List can be used to issue PIV-I Cards. Software and Hardware on the FIPS 201 Approved Products List have been tested to ensure that they can issue or read PIV Cards. While there are slight differences with PIV-I (e.g., a required UUID), the FIPS 201 Approved Products List provides some assurance that the software and hardware will interoperate with PIV-I.

2.23 How are PIV-I Cards and components tested?

PIV-I Cards have to be on the FIPS 201 Approved Products List, which requires NIST SP 800-85A and security testing according to FIPS 140-2. It is recommended that issuers apply the GSA FIPS 201 Evaluation Program Test Tools to a sampling of their issued cards on an ongoing basis to ensure interoperability.

2.24 Is Symmetric Card Authentication Key (CAK) prohibited?

No. However, X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) requires PIV-I Cards to contain an asymmetric CAK. Therefore, the card must be capable of supporting multiple CAKs in order to use a symmetric CAK.

While FIPS 201 allows a PIV Card's Card Authentication Key (CAK) to be either a symmetric (secret) key or an asymmetric private key for physical access, this has resulted in issues associated with PACS interoperability (note that NIST SP 800-116 "strongly recommends that agencies use the asymmetric CAK protocol, rather than a symmetric CAK protocol, whenever the CAK authentication mechanism is used with PACS.")

2.25 What biometrics must be in a PIV-I Card?

PIV-I Card biometric requirements match those of the PIV Card. NIST SP 800-73 requires the biometrics data object to be on the card. NIST SP 800-76 defines the biometrics data object. Specifically, two fingerprint templates, and a digitized photo template are required for PIV-I. A printed photo is also required to be on the card.

2.26 What is the relationship between FASC-N and GUID?

Both the GUID and the FASC-N are data fields within the Cardholder Unique ID (CHUID) per NIST SP 800-73 Part 1. The GUID is included in the CHUID. PIV-I NFI describes the challenges with the FASC-N as follows:

> "The PIV Card includes a Federal Agency Smart Credential - Number (FASC-N) to uniquely identify it, and thus avoid identifier namespace collisions. When managed and distributed within a closed system (the U.S. Government), uniqueness is ensured. However, the FASC-N structure does not support its use beyond the U.S.

> Government as it cannot be easily extended to allow sufficient identifier namespace to support a large NFI population."

The GUID field is defined to contain an RFC 4122-conformant UUID value to support large NFI populations.

2.27 What is the GUID?

The GUID is a mandatory data field defined within the Cardholder Unique ID (CHUID) as specified in NIST SP 800-73 Part 1. PIV and PIV-I Card must conform to NIST SP 800-73. For PIV-I Cards, the GUID field must contain an RFC 4122-conformant UUID value to support large NFI populations.

2.28 What is the relationship between GUID and UUID?

The Global Unique Identification Number (GUID) is a Tagged Length Value (i.e., a structured field) within the CHUID object of a PIV Card. The GUID is defined in NIST SP 800-73 Part 1.

The Universally Unique IDentifier (UUID) is a unique identifier that can be placed in multiple data fields to uniquely identify the card. For example, the UUID is found in the GUID field of the CHUID, the subjectAltName extension of PIV-I Authentication and PIV-I Card Authentication certificates, and within signed objects on the card (in place of the FASC-N in PIV Cards). The UUID is defined in RFC 4122.

On PIV Cards, the GUID may contain a UUID, an IPv6 address, or be populated with all zeros. On PIV-I Cards, the GUID must contain a UUID. Both the UUID and IPv6 addresses provide a unique numbering scheme. However, the UUID does not require a central organization to manage the namespace.

2.29 Where else does the GUID's UUID value appear?

For NFIs, the UUID value that is present in the GUID is present in other data objects as well. For example, the UUID must be present in all objects on a PIV-I credential that would otherwise contain the FASC-N when the card is issued by a Federal issuer. In addition, the UUID must appear in the subjectAltName extension of the PIV-I Authentication and PIV-I Card Authentication certificates as a Uniform Resource Identifier (URI). The UUID also appears in a serialNumber attribute in the subject field of PIV-I Card Authentication certificates where it is encoded using the string representation from RFC 4122.

2.30 What is the format of the UUID in certificates?

The Uniform Resource Name (URN)-formatted value of the UUID is included in the subjectAltName extension of the PIV-I Authentication and PIV-I Card Authentication certificates. One of the defined types of subjectAltName extension is uniformResourceIdentifier. The uniformResourceIdentifier type is used to house the URN-formatted UUID. RFC 4122 defines a method for representing the UUID as a URN.

The UUID also appears in a serialNumber attribute in the subject field of PIV-I Card Authentication certificates where it is encoded using the string representation from RFC 4122.

2.31 Why has the IPv6 GUID value been deprecated in favor of UUID?

The American Registry for Internet Numbers (ARIN) guidance indicates that IPv6 addresses should only be used for internet addressable end points. The RFC 4122 provides a unique numbering scheme that does not require any central organization managing the namespace.

2.32 Where does the GUID appear?

The GUID is a type-length-value (TLV) (i.e., data field) of the CHUID. As such, it only appears in the CHUID. The UUID value that is contained in the GUID is used in other data fields throughout the PIV-I credential.

2.33 Where does the FASC-N appear on the PIV-I Card?

The FASC-N is a unique number for Federal issuers that links all digitally-signed objects into a single credential set in a PIV Card - but not a PIV-I Card. For NFIs, the FASC-N is only contained in a TLV of the CHUID and it must contain 14 nines (9). For PIV-I cards, the UUID links all digitally-signed objects into a single credential set. See NIST SP 800-73 Part 1 for more information.

2.34 Where are the detailed specifications for UUID formatting?

NIST SP 800-73 Part 1 Section 3.3 provides the requirements for formatting the UUID in objects that must contain a UUID.

2.35 Where are the detailed specifications for the value of the FASC-N?

The detailed specifications for the data value of the FASC-N are provided in NIST SP 800-73 Part 1.

2.36 What are the values of the Agency Code of the FASC-N?

The Agency Code for Federal issuers is assigned to each Department or Agency by NIST SP 800-87. The Agency Code for NFIs is 9999. See FAQ 2.40 for contents of the FASC-N in NFI cards.

2.37 Where are the detailed specifications for FASC-N formatting?

FIPS 201 provides the requirements for encoding the FASC-N in certificates and the signed attributes field of CMS-signed objects. NIST SP 800-73 Part 1 provides the requirements for formatting the FASC-N in objects that must contain a FASC-N. NIST SP 800-73 refers to the Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems version 2.2. Note that content of the FASC-N is different for NFIs than for Federal agencies.

2.38 How does a PACS interpret a Federal PIV Card if the card contains a GUID that is all zeros?

The NFI PACS should use the FASC-N values for the Federal PIV card to identify the cardholder.

2.39 How does a Federal PACS interpret an NFI PIV-I Card that does not have a FASC-N?

NFI cards have a FASC-N that contains 14 nines (9). However, the FASC-N is not a unique identifier for NFIs. The GUID is the NFI unique identifier. When a Federal PACS system is reading the CHUID it will have both the FASC-N and the GUID available to it. When the FASC-N contains 14 nines (9), and if technically feasible, the Federal PACS should look for and use the GUID value to identify the cardholder.

2.40 What are the implications of the possible values of a FASC-N and what are the implications to my PACS?

	FASC-N Value	Determination from FASC-N	Issues / Impact
1	Valid Agency / Code System Code Credential Number (CRED#)	• Federal issuer • FASC-N in all required spaces • GUID may be zeros or populated	No impact to Federal PIV cardholders and Federal PACS that key off of FASC-N PACS that only key off of GUID may not receive a GUID from the card – won't interoperate
2	9999 9999 999999	• NFI • GUID contains a UUID • UUID is mandatory in all required spaces • FASC-N not present outside of CHUID	PACS that only key off of FASC-N cannot be used – need to upgrade

2.41 As an Issuer, when do I use the FASC-N versus GUID?

When issuing PIV-I credentials, NFIs are required to populate the UUID and GUID according to NIST SP 800-73 Part 1, in addition to placing 14 nines (9) in the FASC-N. See FAQ 2.26 through 2.43 for related information.

2.42 As a Relying Party, when do I use the FASC-N versus GUID?

For CHUID-based authentication, if the FASC-N is populated with 14 nines (9), the relying party can reasonably conclude it is a PIV-I card and should refer to the GUID for the UUID. For certificate-based authentication, if the subjectAltName does not contain a FASC-N, the relying party can reasonably conclude it is a PIV-I card and should use the UUID from the subjectAltName.

The unique identifier for Federal cards is the FASC-N. The FASC-N is in the subjectAltName extension of the authentication certificate(s) and in the CHUID. See NIST SP 800-73 Part 1 for more information about the FASC-N.

The unique identifier for NFI cards is the UUID. The UUID is in the subjectAltName extension of the authentication certificates, and in the GUID within the CHUID. See FAQs 2.28-2.32 for more information about the UUID.

2.43 How does a PACS determine whether a card is PIV or PIV-I?

The method depends upon the object on the card that is being used to authenticate the cardholder.

Authentication Certificate: PIV cards will validate against id-fpki-common-authentication (2.16.840.1.101.3.2.1.3.13). PIV-I cards will validate against id-fpki-certpcy-pivi-hardware (2.16.840.1.101.3.2.1.3.18).

Card Authentication Certificate: PIV cards will validate against id-fpki-common-cardAuth (2.16.840.1.101.3.2.1.3.17). PIV-I cards will validate against id-fpki-certpcy-pivi-cardAuth (2.16.840.1.101.3.2.1.3.19).

Content Signing Certificate: PIV cards will validate against id-fpki-common-devices (2.16.840.1.101.3.2.1.3.8). PIV-I cards will validate against id-fpki-certpcy-pivi-contentSigning (2.16.840.1.101.3.2.1.3.20).

CHUID: PIV-I Non-Federal cards contain 14 nines (9) in the FASC-N. Federal PIV cards will have a Federal agency code in the FASC-N.

2.44 How do I generate a GUID?

For PIV-I Cards, a GUID is generated using the UUID specification defined in RFC 4122. NIST SP 800-73 Part 1 recommends using algorithm versions 1, 4, and 5 to generate the UUID.

2.45 Are there unique identifier collision issues with NFI Cards?

No. The FASC-N identifier in a PIV-I NFI is not unique and therefore must not be used. There is an extremely low probability of collision for NFI UUID values.

2.46 Are other fields in the FASC-N, such as Person Identifier, defined for NFI Cards?

Neither policy nor specifications provide guidance in this area. Issuers can do anything they like with Person Identifier or the remaining fields of the FASC-N. Therefore, Relying Parties should not make any assumptions regarding format or content of the Person Identifier or the remaining fields of the FASC-N.

3. References

What authoritative documents should I read to successfully implement PIV-I?

3.1 Personal Identity Verification Interoperability for Non-Federal Issuers[9]

Version 1.0.0, May 2009. 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 (1) Common terminology for identity cards, (2) Technical requirements, (3) Identifier namespace, and (4) Trusted identity.

3.2 X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)

Version 2.1.7, June 10, 2010. Defines ten certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between the FBCA and other Entity PKI domains. The policies represent six different assurance levels (Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High) for public key certificates. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

3.3 X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework

Version 1.10, April 8, 2010 – includes six distinct certificate policies: (1) a policy for users with software cryptographic modules, (2) a policy for users with hardware cryptographic modules, (3) a policy for devices, (4) a high assurance user policy, (5) a user authentication policy, and (6) a card authentication policy. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all six policies. The user policies apply to certificates issued to Federal employees, contractors, and other affiliated personnel for the purposes of authentication, signature, and confidentiality. This CP was explicitly designed to support access to Federal systems that have not been designated national security systems.

3.4 X.509 Certificate and CRL Extensions Profile for PIV-I Cards

Version 1.0 April 23, 2010 specifies the X.509 version 3 certificate and version 2 certificate revocation list (CRL) profiles for certificates and CRLs issued under the X.509 Certificate Policy for Federal Bridge Certification Authority (FBCA) for PIV-I. The profiles serve to identify unique parameter settings for certificates and CRLs issued under this policy.

3.5 X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program

January 7, 2008. Specifies the X.509 version 3 certificate and version 2 certificate revocation list (CRL) profiles for certificates and CRLs issued under the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. The profiles serve to identify unique parameter settings for certificates and CRLs issued under this policy.

[9] Approved FBCA Certificate Policy supersedes this document.

3.6 Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile, October 12, 2005

Specifies the X.509 version 3 certificate and version 2 certificate revocation list (CRL) profiles for Federal Public Key Infrastructure (FPKI) systems. The profiles serve to identify unique parameter settings for FPKI systems. In order to maximize interoperability among PKI communities within the Federal government, this profile was designed to complement the NIST Recommendation for X.509 Path Validation. The NIST Recommendation specifies a minimum set of features from X.509 that path validation software must implement in order to be considered a Bridge-enabled Path Validation Module (PVM). This profile recommends against the use of features from X.509 that are not included in this minimum set.

3.7 Security Requirements for Cryptographic Modules, FIPS 140-2

May 25, 2001. Specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

3.8 Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-1

Defines a reliable, government-wide PIV system for use in applications such as access to Federally-controlled facilities and information systems. This standard has been developed within the context and constraints of Federal law, regulations, and policy based on information processing technology currently available and evolving. This standard specifies a PIV system within which common identification credentials can be created and later used to verify a claimed identity. The standard also identifies Federal government-wide requirements for security levels that are dependent on risks to the facility or information being protected.

3.9 Interfaces for Personal Identity Verification (4 Parts), NIST SP 800-73-3

Interfaces for Personal Identity Verification (4 parts): (1) End-Point PIV Card Application Namespace, Data Model and Representation, (2) PIV Card Application Card Command Interface, (3) PIV Client Application Programming Interface, and (4) PIV Transitional Interfaces and Data Model Specification

3.10 Biometric Data Specification for Personal Identity Verification, NIST SP 800-76-1

January 2007. Contains technical specifications for biometric data mandated in FIPS. These specifications reflect the design goals of interoperability and performance of the PIV Card. This specification addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The goals are addressed by citing biometric standards normatively and by enumerating requirements where the standards include options and branches. In such cases, a biometric profile can be used to declare what content is required and what is optional. This document goes further by constraining implementers' interpretation of the standards. Such restrictions are designed to ease implementation, assure conformity, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications. The biometric data specification in this document is the mandatory format for biometric data carried in the PIV Data Model (Appendix A of **NIST SP 800-73-3**). Biometric data used only outside the PIV Data Model is not within the scope of this standard.

3.11 Cryptographic Algorithms and Keys Sizes for Personal Identity Verification, NIST SP 800-78-2

February 2010. Contains the technical specifications needed for the mandatory and optional cryptographic keys specified in **FIPS 201** as well as the supporting infrastructure specified in **FIPS 201** and the related **NIST SP 800-73-3**, *Interfaces for Personal Identity Verification*, and **NIST SP 800-76**, *Biometric Data Specification for Personal Identity Verification*, that rely on cryptographic functions.

3.12 PIV Data Model Test Guidelines, NIST SP 800-85B

July 2006. Targeted at vendors and integrators of PIV components, as well as the entities that will conduct tests on such components. Readers are assumed to have a working knowledge of **FIPS 201**, PIV guidance, and applicable technologies. This document will: 1. Enable developers of PIV components to develop their modules to be testable for requirements specified in **FIPS 201**, **NIST SP 800-73**-3, **NIST SP 800-76**, and **NIST SP 800-78**, 2. Enable developers of PIV components to develop self-tests as part of the development effort, and 3. Enable testers to develop tests that cover the test suite provided in this document.

3.13 PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 compliance), NIST SP 800-85A, March 2009

Test guidance document specifies the test plan, processes, derived test requirements, and the detailed test assertions/conformance tests for testing the following PIV software components: (1) PIV middleware (implements PIV Client API), and (2) PIV card application.

3.14 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), NIST SP 800-116

November 2008. Describe a strategy allowing agencies to PIV-enable their PACS, and migrate to government-wide interoperability. Specifically, the document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to Federal government facilities and assets. With the intent to facilitate and encourage greater use of PIV Cards, this document: (1) Describes the desired characteristics of a target implementation of PIV-enabled PACS, (2) Describes trust and infrastructure challenges that must be overcome to achieve government-wide credential interoperability, (3) Discusses the PIV Card capabilities so that risk-based assessment can be aligned with the appropriate PIV authentication mechanism, (4) Recommends to Federal agencies an overall strategy for the implementation of PIV authentication mechanisms with agency facility PACS, and (5) Proposes a PIMM to measure the progress of facility and agency implementations. This document focuses on the use of PIV Cards to gain access to Federal buildings and facilities. This document does not address non-PIV authentication mechanisms.

3.15 FIPS 201 Approved Products List

Dynamic list that only lists those products and services that are in conformant to the current version of the Standard and its supporting Publications.

3.16 RFC 4122, Universally Unique Identifier (UUID) URN Namespace

Defines a Uniform Resource Name namespace for UUIDs (Universally Unique IDentifier). A UUID is 128 bits long, and can guarantee uniqueness across space and time.

3.17 Electronic Authentication Guideline, NIST SP 800-63

Provides technical guidance to agencies to allow an individual person to remotely authenticate his/her identity to a Federal IT system. This guidance addresses only traditional, widely implemented methods for remote authentication based on secrets. With these methods, the individual to be authenticated proves that he or she knows or possesses some secret information.