hspd12

Personal Identity Verification Interoperability

For

Non-Federal Issuers

Issued by Federal CIO Council

May 2009

Executive Summary

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 Card (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:

1. **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;
2. **Technical requirements** – for non-federally issued identity cards to interact with federal infrastructure, basic technological requirements must be met;
3. **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
4. **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.

Federal agency trust of non-federally issued identity cards is not mandated. Instead, a set of minimum requirements for enabling trust is provided. Using appropriate mechanisms (e.g., risk assessment), each federal agency decides for itself which, if any, non-federally issued identity cards to trust – and if so, for what purposes.

For additional information concerning this document, please contact icamsc@gsa.gov.

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.

Several federally sponsored programs in this regard already exist and use NFIs. The programs include First Responder Authentication Credential (FRAC), Transportation Worker Identity Credential (TWIC), and Airport Credential Interoperability Solution (ACIS). Many other programs are in development with the same desired goal of being technically interoperable and trustworthy in the Federal government PIV environment.

1.2 Scope

This document is limited to describing NFI identity cards that can be interoperable with the Federal government PIV systems and can be trusted by Federal government relying parties.

1.3 Document Objectives

This document provides solutions for overcoming the barriers to federal reliance on non-federal identity cards. Four specific areas of concern have been identified:

1. **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;
2. **Technical requirements** – for non-federally issued identity cards to interact with federal infrastructure, basic technological requirements must be met;
3. **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
4. **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.

For each of these, a minimum set of requirements has been described that will allow NFI identity cards to technically interoperate with Federal government PIV systems and be trusted by Federal government relying parties.

2. MINIMUM NFI CARD REQUIREMENTS

Federal government reliance (trust) on NFI identity cards requires the card to technically comply with PIV specifications so as to technically interoperate with Federal government PIV systems, and to have specific trust elements. The following sub-sections explain how to meet those requirements.

2.1 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. A major issue in the identity card space is the lack of standard terminology to unambiguously distinguish between characteristics (e.g., trust characteristics) of federally issued and NFI identity cards. The result can be confusion, uncertainty, or misunderstanding regarding the capabilities and trustworthiness an identity card encompasses – particularly an NFI identity card. Attaining clarification after the fact can be costly in many ways (e.g., investing and implementing with an incorrect understanding likely requires rework or abandonment). PIV standards clearly define the federally issued PIV Card. However, the definition of different NFI identity cards, especially regarding their relationship to PIV remains problematic. This document resolves the terminology problem by proposing a more complete set of identity card terms that unambiguously describes federal and NFI identity cards in terms of critical characteristics affecting the degree of federal relying party trust. The proposed terms are:

- **PIV Card** – an identity card that is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure that PIV Cards are interoperable with and trusted by all Federal government relying parties.
- **PIV Interoperable Card** – an identity card that meets the PIV technical specifications to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal government relying parties to trust the card.
- **PIV Compatible Card** – an identity card that meets the PIV technical specifications so that PIV infrastructure elements such as card readers are capable of working with the card, but the card itself has not been issued in a manner that assures it is trustworthy by Federal government relying parties.

A PIV Interoperable Card builds upon a PIV Compatible Card. An NFI must procure a PIV Compatible Card and issue it in a trustworthy manner. NFI PIV Compatible Cards and NFI PIV Interoperable Cards are not PIV Cards because NFIs and their identity cards cannot directly meet certain Federal government PIV requirements.

An NFI PIV Compatible Card is not a PIV Interoperable Card. An NFI PIV Interoperable Card can be trusted by Federal government relying parties because it has the minimum set of PIV trust elements. An NFI PIV Compatible Card cannot be trusted by Federal government relying parties because it lacks the minimum set of PIV trust elements.

2.1.1 Assumptions

The following assumptions apply:

1. Each Federal government relying party determines the extent to which it will trust PIV Interoperable Cards within its areas of control;
2. Cardholder privileges in any particular situation are determined solely by the Federal government relying party (i.e., PIV Interoperable Cards do not guarantee access of any kind, nor do they prevent issuance of a PIV Card); and
3. Each Federal government relying party makes access decisions based on the ability to verify the validity of the PIV Interoperable Card and on local access policy for external organizations.

2.1.2 Requirements

The following requirements apply to NFIs:

1. NFI PIV Compatible Cards and NFI PIV Interoperable Cards will use a smart card platform that is technically compatible with National Institute of Standards and Technology (NIST) technical requirements outlined in Section 2.2 of this document;
2. Consistent with the policy directives in Office of Management and Budget (OMB) memorandum M-05-24, NFI PIV Compatible Cards and NFI PIV Interoperable Cards should contain distinctive markings indicating the identity of the issuing entity; and
3. NFI PIV Interoperable Cards are electronically personalized, as defined by FIPS 201 and supporting documents.
    a. NFI PIV Interoperable Cards will include an Authentication Digital Public Key Infrastructure (PKI) certificate that meets a minimum set of criteria identified in Section 2.4 of this document.
    b. NFI PIV Interoperable Cards will include biometric fingerprint information that conforms to NIST Special Publication (SP) 800-76.

2.2 Technical Requirements

For non-federally issued identity cards to interact with federal infrastructure, basic technological requirements must be met. NFI identity cards must conform to the NIST technical specifications for a PIV Card as defined in NIST SP 800-73 and meet the cryptographic requirements of FIPS 140 and NIST SP 800-78. In order to ensure this conformance, NFIs should refer to the General Services Administration (GSA) Approved Products List (APL) available at www.idmanagement.gov. See Appendix A for additional technical information.

2.2.1 Required Electronic Features

NFI PIV Interoperable Cards must be populated in accordance with NIST SP 800-73[1] and contain, at a minimum, the following:

- Biometric;
- Card Holder Unique Identifier (CHUID); and
- Authentication PKI Certificate[2].

NFIs are encouraged to support the Card Authentication Key (CAK) per NIST SP 800-116, "NIST strongly recommends that every PIV Card contain an asymmetric CAK and corresponding certificate and that PACS use an asymmetric challenge/response CAK protocol".

2.2.2 Required Physical Features

The physical topography of NFI PIV Interoperable Cards must include, at a minimum, the following:

- Issuing/Sponsoring Organization (e.g. Company name);
- Card holder Photograph;
- Card holder Full Name; and
- Card Expiration Date.

NFI PIV Interoperable and Compatible Card visual distinction is recommended to ensure no suggestion of attempting to create a fraudulent PIV Card.

[1] PIV Interoperable objects should conform to SP 800-73, with the exception of the extensions/modifications identified in this NFI document

[2] The Authentication PKI Certificate is functionally similar to the PIV Authentication Certificate, requiring card holder authentication (e.g., PIN) to the cryptographic module before activation of the private key.

2.3 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. 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. In addition, NFIs cannot consistently assign globally unique FASC-Ns. Consequently, there is a need to develop a Smart Card Numbering scheme comparable to the FASC-N that follows a set of guidelines that ensure uniqueness across the federal issuers and NFIs.

2.3.1 Use of the GUID Field by NFIs

The CHUID Global Unique Identifier (GUID) field is best suited for uniquely identifying identity cards across federal issuers and NFIs. NFIs shall include a valid RFC 4122 generated GUID. In addition, NFIs should include the GUID in a subject-alt-name extension of the authentication certificate to ensure GUID availability to relying parties in remote Logical Access Control System (LACS) environments. In the near future, Federal PKI standards are expected to require use of the GUID in subject-alt-name extensions for federal and non-federal issuers.

2.3.2 Use of the FASC-N Field by NFIs

NFIs must generate and use a FASC-N in all locations required by NIST SP 800-73 and NIST SP 800-76[3]. The following text from *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* v2.2, referenced by NIST SP 800-73, establishes FASC-N construction rules for NFIs:

> "*The FASC-N is not designed to insure uniqueness for non-federal issuers. For non-federal issuers, additional tag length value (TLV) elements must be specified to insure uniqueness of the FASC-N. If an Agency Code of 9999 is present in the FASC-N, then the DUNS TLV record in the CHUID container will indicate the identity of the card issuer. It is anticipated that the Tag 30 TLV record will always exist for industry compatibility for PACS that use the System Code and Card Number as a card identifier.*
>
> *For issuers not defined in SP 800-87, a FASC-N can be constructed using an Agency Code of 9999; however, this will not provide uniqueness of the FASC-N for federal agency applications. If a non-federal issuer has a requirement for federal interoperability, then a sponsoring agency may assign a specific System Code(s) to the issuer. When an Agency Code of 9999 is specified, an issuer must include an additional TLV record in the CHUID, such as the DUNS, to insure*

Federal government relying parties can distinguish NFI PIV Interoperable cards through the 9999 value in the FASC-N.

[3] Future revisions of NIST SP 800-73 and NIST SP 800-76 are expected to further specify the use of the GUID.

uniqueness of the CHUID. It is the responsibility of the sponsoring agency to maintain records of specific System Code assignments for both internal and external issuers of FASC-Ns".

The above rules create a serious identifier namespace collision risk about which relying parties should be aware. For access control purposes, legacy Physical Access Control System (PACS) often only read fourteen (14) digits consisting of the agency code, system code, and credential number. The FASC-N rules for NFIs do not ensure uniqueness for those fourteen digits across issuers, creating the potential for two different people having the same identifier for legacy PACS. Federal government relying parties are encouraged to consider this issue and make local risk-based decisions regarding NFI PIV Interoperable Cards and their legacy PACS.

If a Federal government relying party PACS is capable of processing NFI Interoperable Cards, the GUID should be relied upon as a unique card identifier. Otherwise, the Federal government relying party should consider alternative risk-based solutions.

2.4 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. To trust any identity card, it must be possible to validate the card (i.e., not expired, not revoked) and authenticate the cardholder (i.e., the cardholder is who he or she says he or she is). The PIV Authentication Certificate is where "trust" in the PIV Card resides. However, the policy object identifier (OID) for the PIV Authentication Certificate is available only to Federal government organizations. Therefore, a comparable Identity PKI Authentication Certificate that can be trusted by Federal government relying parties must be identified and used by NFIs.

In addition, trust in an identity card requires an understanding and acceptance of the process used to determine the accuracy of the claimed identity. For the Federal government PIV Card, FIPS 201 specifies identity proofing and background vetting processes. While NFIs are unable to mirror the background vetting process (e.g., the National Agency Check with Written Inquiries (NACI)) employed by the Federal government, they can and must perform identity proofing in a manner that promotes trust in the process. Accordingly, NFIs require a common identity proofing standard that is understood by and acceptable to the Federal government.

2.4.1 NFI Identity Authentication PKI Certificate

NFI PIV Interoperable Cards must include an Identity Authentication PKI Certificate issued by a Certification Authority (CA) that chains to the Federal Bridge Certification Authority (FBCA) at the Medium Hardware assurance level via cross-certification. This will enable Federal government relying parties to verify the validity of the identity card via the Identity Authentication PKI Certificate by first verifying the issuing organization (i.e., CA cross-certified with FBCA), and then providing assurance that the certificate (and by extension, the card) has not been revoked or invalidated since issuance.

The Identity Authentication PKI Certificate in an NFI PIV Interoperable Card contains a policy OID other than the one mandated for Federal PIV Authentication use, which contributes to satisfying the electronic distinctiveness requirement for the NFI PIV Interoperable Card.

2.4.2 Ensuring Identity Validity

The Federal government's identity proofing and background vetting processes, as defined in FIPS 201, are two distinct activities.

2.4.2.1 Identity Proofing

During identity proofing, the applicant is required to appear in person and provide two forms of identity source documents in original form from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, *Employment Eligibility Verification*. At least one of the documents must be a valid State or Federal government-issued picture identification (ID). This identity proofing process is commensurate with OMB Memorandum M-04-04, *E-Authentication*

Guidance for Federal Agencies, Assurance Level 4, which in turn provides the common identity proofing standard for NFIs.

NIST SP 800-63 defines E-Authentication Assurance Level 4 identity proofing as:

- In-person appearance and verification of two independent ID documents or accounts, one of which must be a current primary government picture ID that contains the applicant's photograph and either their address of record or nationality (e.g. driver's license or passport), and a new recording of a biometric of the applicant at the time of application.
- The Registration Agent must inspect the primary Photo-ID and if apparently valid, compare picture to applicant, record ID number, address and date of birth (DoB). If available, a digital image of the Photo-ID shall be captured and stored.
- The Registration Agent must inspect secondary government ID or financial account, and if apparently valid, compare picture to applicant, record ID number, address and DoB, or verify financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirm that: name, DoB, address, and other personal information in records are consistent with the application and sufficient to identify a unique individual.
- The Registration Agent records a current biometric (e.g. photograph, fingerprints) to ensure that applicant cannot repudiate application and issues cards in a manner that confirms address of record.

In addition to its role in ensuring the validity of an identity card, the FBCA Medium Hardware assurance level Identity Authentication PKI Certificate ensures that the NFI meets E-Authentication Assurance Level 4 identity proofing. As a result, Federal government relying parties can trust the asserted identity of the NFI PIV Interoperable Card holder.

2.4.2.2 Background Vetting Process

The Federal background vetting process (e.g. NACI) is performed in order to determine an individual's suitability/fitness to work for or on behalf of the Federal government and is not applicable to NFI identity cards.

For purposes of PIV interoperability, NFIs need to concern themselves only with satisfying the identity proofing requirements for E-Authentication Assurance Level 4. Where suitability/fitness is a concern for an agency, the agency may require further background checks for access (however, this is outside the scope of this document).

Federal government relying parties continue to be responsible for validating the Authentication PKI Certificate, authenticating cardholder identity, and managing individual cardholder roles and authorizations.

APPENDIX A: TECHNICAL INFORMATION

This Appendix provides additional technical information in support of Section 2.2, Technical Requirements. The following table provides a comparison of the requirements for each card type.

		PIV Card	PIV Interoperable	PIV Compatible
Suitability	National Agency Check (NAC) prior to issuance	●		
	NACI	●		
Trust	FIPS 201 Conformant	●		
	PIV OID on PIV Authentication Certificate (trust model)	●		
	Medium Hardware equivalent Authentication Certificate[4]	●	●	
	Medium Hardware equivalent object signing certificate	●	●	
Card Edge	Card Stock on GSA APL[5]	●	●	●
	PIV Application Identifier (AID)	●	●	●
	Command edge and NIST SP 800-85 conformant[6]	●	●	●
	PKI certificate profile compliant with Federal Common Policy[7]	●	●	●
	NIST SP 800-73 conformant GUID present in the CHUID	●	●	●
	RFC 4122 conformant GUID required in the CHUID[8]		●	●
	RFC 4122 conformant GUID present in the Authentication Certificates[9]		●	●
	Visually distinguishable from PIV Card		●	●

[4] Certificate equivalence for NFIs is established by the FBCA.

[5] Conformant form factor.

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

[7] PKI certificates on PIV Compatible credentials do not link back to the federal bridge, but the certificates must be created with the correct certificate profile for the type of certificate being used.

[8] 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. Future revisions of NIST SP 800-73 are expected to address this requirement for PIV cards.

[9] The GUID will be in the subject-alt-name of the PIV Authentication Certificate and the Card Authentication Certificate. Future Federal Public Key Infrastructure Policy Authority (FPKIPA) guidance is expected.

The PIV Card provides multiple authentication mechanisms[10] including:

- **Authentication Certificate** – allows PKI-based authentication only accessible via the contact interface when the user Personal Identification Number (PIN) is provided;
- **Biometric**[11] – authentication of the cardholder's fingerprints using biometric templates on the card, including verification of the signature and signer;
- **Cardholder Unique Identifier (CHUID)** – contactless read of the CHUID object, including verification of the signature and signer; and
- **Card Authentication Key (CAK)** – provides flexible card authentication options that may be performed via the contactless interface.

Each authentication method must conform to certain PIV data model elements defined in the following NIST SPs:

- **NIST SP 800-73** – provides PIV Card technical interoperability specifications. PIV Compatible Cards and PIV Interoperable Cards must adhere to the NIST SP 800-73 data model and card edge requirements;
- **NIST SP 800-76** – provides PIV Card biometric technical guidance. PIV Interoperable Cards must capture and store biometrics on the card in accordance with NIST SP 800-76; and
- **NIST SP 800-78** – provides PIV Card technical guidance regarding digital credentials present on the PIV Card. This is where much of the trust in the identity credential will be established. PIV Interoperable Cards must ensure their digital credentials meet NIST SP 800-78 technical requirements and the requirements discussed in Section 2.3.

[10] For more information on these methods, see FIPS 201, section 6.2.

[11] Biometric data is accessible only after providing the correct PIN and only via the contact interface.

As of the date of this document, PACS Implementation Guidance defines the PIV CHUID as follows:

Data Element	Max Bytes	Description
Buffer Length	2	Mandatory TLV record. Exists when a TLV record in addition to the FASC-N exists in the CHUID for contact File System and contact-less smart cards. The Buffer Length TLV record is defined in GSC-IS Section 8.3.
FASC-N	25	Mandatory TLV Record. Federal Agency Smart Credential Number is defined in Section 6 of this document.
Agency Code	4	Optional TLV Record. Recommended when the SP 800-87 code for the government agency issuing the credential contains alpha characters.
Organizational Identifier	4	Optional TLV Record. Recommended when the SP 800-87 code for the FASC-N OI field contains alpha characters.
DUNS	9	Optional TLV Record. Recommended when the FASC-N Agency Code = 9999. D&B DUNS number for non-federal FASC-N issuer.
GUID	16	Mandatory TLV Record. A registered IPv6 address allocated to the CIO's office by ARIN and unique to the card.
Expiration Date	8	Mandatory TLV Record. Card expiration date, YYYYMMDD
Authentication Key MAP	512	Optional TLV Record. May exist for High Assurance Profile applications.
Asymmetric Signature	2816	Mandatory TLV Record. Issuer defined algorithm, public key and signature.
LRC	1	Optional TLV Record Longitudinal Redundancy Code.

As of the date of this document, PACS Implementation Guidance defines the PIV FASC-N as follows:

Field Name	Length (BCD Digits)	Field Description
Agency Code	4	Identifies the government agency issuing the credential.
System Code	4	Identifies the system the card is enrolled in and is unique for each site.
Credential Number	6	Encoded by the issuing agency. For a given system no duplicate numbers are active.
CS	1	CREDENTIAL SERIES (SERIES CODE) Field is available to reflect major system changes.
ICI	1	INDIVIDUAL CREDENTIAL ISSUE (CREDENTIAL CODE) Recommend coding as a "1" always.
PI	10	PERSON IDENTIFIER Numeric Code used by the identity source to uniquely identify the token carrier. (e.g. DoD EDI PN ID, TWIC credential number, NASA UUPIC).
OC	1	ORGANIZATIONAL CATEGORY 1 - Federal Government Agency 2 - State Government Agency 3 - Commercial Enterprise 4 - Foreign Government
OI	4	ORGANIZATIONAL IDENTIFIER OC=1 – NIST SP800-87 Agency Code OC=2 – State Code OC=3 – Company Code OC=4 – Numeric Country Code
POA	1	PERSON/ORGANIZATION ASSOCIATION CATEGORY 1 – Employee 2 – Civil 3 – Executive Staff 4 – Uniformed Service 5 – Contractor 6 – Organizational Affiliate 7 – Organizational Beneficiary
SS	1	Start Sentinel. Leading character which is read first when card is swiped.
FS	1	Field Separator.
ES	1	End Sentinel.
LRC	1	Longitudinal Redundancy Character.

APPENDIX B: GLOSSARY

Term	Definition
Access Control	The process of granting or denying requests to access physical facilities or areas, or logical systems (i.e., computer networks or software applications). See also "logical access control system" and "physical access control system."
Authentication	The process of establishing confidence in the identity of users or information systems.
Authorization	The process of giving individuals access to specific areas or systems based on their authentication.
Biometric	A measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints and facial images. A biometric system uses biometric data for authentication purposes.
Cardholder Unique Identifier (CHUID)	The PACS Implementation Guidance [PACS] defines the CHUID data object; this description is refined in NIST SP 800-73. The PIV Card shall include the CHUID as defined in NIST SP 800-73. The CHUID includes an element, the Federal Agency Smart Credential - Number (FASC-N), which uniquely identifies each card. CHUID elements specific to this standard are described below in Section 4.2.1. The format of the CHUID signature element is described in Section 4.2.2. The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV Card without card activation. The PIV FASC-N shall not be modified post-issuance.
Constituent	Member of a group or organization.
FBI Fingerprint Check	Fingerprint check of the FBI fingerprint files. This check is an integral part of the NACI, and is the minimum requirement for provisional PIV Card issuance.
Federal Agency Smart Credential Number (FASC-N)	The FASC-N is the primary identification string to be used on all government issued credentials. The key to credibility, non-repudiation and reciprocity is the definition and acceptance of a credential token identification numbering schema for use across all Federal Agencies that is uniquely assigned to one and only one individual. For deployed systems, this is the FASC-N. For emerging systems, it is the GUID. Both are contained in the CHUID for consistent means of access by PACS solutions allowing for ease of migration. The responsibility for issuing this number to federal personnel is decentralized to the various federal agencies, with the ultimate responsibility for ensuring uniqueness residing with each agency's CIO, or other duly designated agency official. For the FASC-N, this is achieved through an assigned Agency Code and subordinate system code and credential number.
Identity Proofing	The process of providing sufficient information (e.g., driver's license, proof of current address, etc.) to a registration authority, or the process of verifying an individual's information that he or she is that individual and no other.

Term	Definition
Logical Access Control System (LACS)	Protection mechanisms that limit users' access to information and restrict access on the system to only what is appropriate for them. These systems may be built into an operating system or application, or may be an added system.
National Agency Check (NAC)	A standard process that involves searches of the Security/Suitability Investigations Index (SSI), Defense Clearance and Investigation Index (DCII), FBI Name Check, and FBI National Criminal History Fingerprint Check.
National Agency Check with Written Inquiries (NACI)	The basic and minimum investigation required for all new federal employees and contractors, which consists of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name, fingerprint files, and other files or indices when necessary. This investigation also includes written inquiries and searches of records covering specific areas of an individual's background during the past five (5) years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes employment (five (5) years); education (five (5) years and highest degree verified); residence (three (3) years); references; law enforcement (five (5) years); and NACs.
Non-Federal Issuer	This is an issuer that wishes to issue identity credentials that are PIV Compatible or PIV Interoperable.
Physical Access Control System (PACS)	Protection mechanisms that limit users' access to physical facilities or areas to only what is appropriate for them. These systems typically involve a combination of hardware and software (e.g., a card reader) and may involve human control (e.g., a security guard).
PIV Card	A government-issued credit card-sized identification that contains a contact and contactless chip. The holder's facial image will be printed on the card, along with other identifying information and security features. The contact chip will store a PKI certificate, the Cardholder Unique Identifier (CHUID), and a fingerprint biometric, all of which can be used to authenticate the user for physical access to federally controlled facilities and logical access to federally-controlled information systems. A PIV Card is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure the PIV Cards are interoperable with and trusted by all Federal government relying parties.

Term	Definition
PIV Compatible Card	An identity card that meets the technical specifications so that PIV infrastructure elements such as card readers are capable of working with the cards, but the card itself has not been issued in a manner that assures it is trustworthy by federal relying parties. A PIV Compatible Card is not sufficient for trust by federal relying parties. Only a PIV Interoperable card can be trusted by a federal relying party – if the federal relying party chooses – because of its additional elements described later in this document. As a result, a PIV Compatible Card is of no value to the Federal government because it does not have all the elements needed for Federal government trust.
PIV Interoperable Card	An identity card that meets the technical standards to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows federal relying parties to trust the cards.
Public Key Infrastructure (PKI)	A service that provides cryptographic keys needed to perform digital signature-based identity verification, and to protect communications and storage of sensitive data.
Registration Agent	A trusted entity that establishes and vouches for the identity of a Subscriber to a CSP. The Registration Agent may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).

APPENDIX C: ACRONYMS

Acronym	Definition
ACIS	Airport Credential Interoperability Solution
AID	Application Identifier
APL	Approved Products List
CA	Certification Authority
CAK	Card Authentication Key
CHUID	Cardholder Unique Identifier
DoB	Date of Birth
DUNS	Data Universal Numbering System
FASC-N	Federal Agency Smart Credential - Number
FBCA	Federal Bridge Certification Authority
FBI	Federal Bureau of Investigation
FICC	Federal Identity Credentialing Committee
FIPS	Federal Information Processing Standard
FPKIPA	Federal Public Key Infrastructure Policy Authority
FRAC	First Responder Authentication Credential
GSA	General Services Administration
GUID	Global Unique Identifier
HSPD-12	Homeland Security Presidential Directive 12
ID	Identification
IP	Internet Protocol
ISO/IEC	International Organization for Standardization / International Electrotechnical Organization
LACS	Logical Access Control System
MAC	Media Access Control
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries

Acronym	Definition
NFI	Non-Federal Issuer
NIST	National Institute of Standards and Technology
NPIVP	NIST Personal Identity Verification Program
NSPD	National Security Presidential Directive
OID	Object Identifier
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PACS	Physical Access Control System
PAIIG	Physical Access Interagency Interoperability Working Group
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	PIV Interoperable
PKI	Public Key Infrastructure
RFC	Requests for Comment
SP	Special Publication
TLV	Tag Length Value
TWIC	Transportation Worker Identity Credential
U.S.	United States
WG	Working Group

APPENDIX D: DOCUMENT REFERENCES

Executive Order 13388: Further Strengthening the Sharing of Terrorism Information to Protect America (October 25, 2005)
http://www.fas.org/irp/offdocs/eo/eo-13388.htm

FIPS 140: Security Requirements for Cryptographic Modules
http://csrc.nist.gov/publications/PubsFIPS.html

FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors
http://csrc.nist.gov/publications/PubsFIPS.html

HSPD-5 Management of Domestic Incidents: Establishes a single, comprehensive national incident management system (February 28, 2003)
http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html

HSPD-6 Integration and Use of Screening Information: Consolidates the government's approach to terrorism screening and information collection and usage in screening processes. (September 16, 2003)
http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html

HSPD-7 Critical Infrastructure Protection, Prioritization, and Protection: Federal departments and agencies are to identify, prioritize, and protect United States critical infrastructure and key resources (December 17, 2003).
http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

HSPD-8 National Preparedness: Defines "first responder" as those who are responsible for the protection and preservation of life, property, evidence, and the environment (December 17, 2003)
http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html

HSPD-11 Comprehensive Terrorist-Related Screening Procedures: Research and development on technologies, including biometric identifier (also Executive Order 13356)
http://www.whitehouse.gov/news/releases/2004/08/20040827-7.html

HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors: Sets a standard for secure and reliable forms of identification
http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

HSPD-16 / NSPD-47: "Aviation Transportation System Security Policy" details a strategic vision for aviation security while recognizing ongoing efforts, and directs the production of a National Strategy for Aviation Security and supporting plans (June 20, 2006)
http://www.dhs.gov/xprevprot/laws/gc_1173113497603.shtm

H.R 418: Real ID Act 2005: Separates driving privilege from identity for state driver's license as of May 2008
http://www.govtrack.us/congress/bill.xpd?bill=h109-418

Intelligence Reform and Terrorism Prevention Act of 2004, Title IV – Transportation Security Section 4011 (December 17, 2004)
http://www.nctc.gov/docs/pl108_458.pdf

NIST SP 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems
http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-63: Electronic Authentication Guideline
http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-73: Interfaces for Personal Identity Verification (4 Parts)
http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-76: Biometric Data Specification for Personal Identity Verification
http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-78: Cryptographic Algorithms and Key Sizes for Personal Identity Verification
http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-79: Guidelines for the Accreditation of Personal Identity (PIV) Verification Card Issuers (PCI's)
http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-104: A Scheme for PIV Visual Card Topology
http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
http://csrc.nist.gov/publications/PubsSPs.html

OMB A-130: Management of Federal Information Resources, 1996
http://www.whitehouse.gov/omb/circulars/a130/a130.html

OMB M-03-22: OMB Guidance for Implementing the Privacy Provisions the E-Government Act of 2002
http://www.whitehouse.gov/omb/memoranda/m03-22.htm)

OMB M-04-04: E-Authentication Guidance for Federal Agencies
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

OMB M-05-05: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services
http://www.whitehouse.gov/omb/memoranda/fy2005/m05-05.pdf

OMB M-05-24: Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf

Request for Comments (RFC) 4122, A Universally Unique Identifier (UUID) URN Namespace
http://www.ietf.org/rfc/rfc4122.txt

Request for Comments (RFC) 3852, Cryptographic Message Syntax (CMS)
http://www.ietf.org/rfc/rfc3852.txt

The Aviation and Transportation Security Act (ATSA), 2001
http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf

Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems v2.3
http://www.smart.gov/iab/documents/PACS.pdf

The E-Government Act, 2002
http://www.archives.gov/about/laws/egov-act-section-207.html

The Electronic Signatures Act, 2000
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s761enr.txt.pdf

The Enhanced Border Security and Visa Entry Reform Act, 2002
http://travel.state.gov/visa/laws/telegrams/telegrams_1403.html

The Government Paperwork Elimination Act (GPEA), 1998
http://www.cio.gov/documents/paperwork_elimination_act.html

The Government Paperwork Reduction Act (PRA), 1995
http://www.archives.gov/federal-register/laws/paperwork-reduction/

The Government Performance and Results Act (GPRA), 1993
http://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m.html

The Homeland Security Act, 2002
http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm

National Strategy for Homeland Security, Office of Homeland Security (OHS), 2002
Twww.dhs.gov/xlibrary/assets/nat_strat_hls.pdf

The Federal Information Security Management Act, 2002
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf

The Privacy Act of 1974
http://www.usdoj.gov/oip/privstat.htm

Title 14, Code of Federal Regulations (CFR), Chapter I, Part 107
http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title14/14tab_02.tpl

Title 49, Code of Federal Regulations (CFR), Chapter XII, Part 1542.209 & 1544.229
http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title49/49tab_02.tpl

USA Patriot Act, 2001
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf