Personal Identity Verification Interoperability

For

Issuers

Version 2.0.1

Approved

July 27, 2017

Revision	Date	Summary of Changes
1.0	July 2010	Original
2.0	November 2016	● Removed most duplicative references to requirements which have been stated in other government documents as authoritative ● Updated references to Memorandums, Standards and common terminology ● Added clarification for federal agencies on the boundaries of security, auditing and procurement requirements
2.0.1	December 2016	● Updated Table 4 to clarify for Legislative and Judicial branches of federal government

Executive Summary

Federal agencies are interested in issuing and acquiring identity credentials and credential services that are not Personal Identity Verification (PIV) credentials, but are (a) technically interoperable with Federal Government PIV infrastructure, and (b) issued in a manner that allows Federal Government relying parties to trust the credentials. The PIV credential standard, Federal Information Processing Standards (FIPS) 201-2, has requirements[1] that only federal agencies can meet to issue PIV credentials, requiring needed guidance for Issuers of PIV-Interoperable credentials. Prior guidance for the issuance of PIV-Interoperable credentials neglected to address the issuance of PIV-Interoperable credentials by federal agencies, requiring additional guidance for all issuers.

This document provides the guidance needed to assist both Federal Issuers and Non-Federal Issuers (NFI) of PIV-Interoperable (PIV-I) identity credentials in achieving credential interoperability with the Federal Government PIV infrastructure. This document's scope is limited to the issuance of PIV-Interoperable credentials; federal departments and agencies must continue to make their own authorization determination to allow or deny access when a PIV-Interoperable credential is used for authentication.

This document advocates a set of minimum requirements for PIV-Interoperable credentials that can be trusted by the Federal Government, and details solutions to the four barriers to interoperability that currently challenge Federal government. These four barriers are as follows:

1. **Common terminology for identity credentials and issuers** – To ensure consistency, a lexicon for differentiating a PIV credential from a credential interoperable with PIV infrastructure, and the differences between Non-Federal and Federal Issuers, has been developed.

2. **Assured identity** – The fundamental purpose of an identity credential is to establish the identity of the credential holder. Therefore, an identity credential must be issued in a federated model and consistent manner which provides the Federal Government with a requisite level of identity assurance.

3. **Technical requirements** – For identity credentials to be interoperable with the federal PIV infrastructure, basic technological requirements must be met.

4. **Security and auditing** – The boundaries for auditing and compliance requirements require clarification for federal agencies.

[1] In particular, these requirements are specified in FIPS 201-2 Section 2.1 Control Objectives, related to adjudication of fitness and suitability, and are common minimum personnel assurance for all federal PIV holders.

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

Table of Contents

1 INTRODUCTION

1.1 Background

The Federal Government's reliance (trust) on PIV credentials establishes a baseline for identity assurance, authenticator assurance, and suitability assurance. Federal agencies and issuers of identity credentials have expressed a desire to produce identity credentials that can be interoperable with Federal Government Personal Identity Verification (PIV) infrastructure and could be trusted by the Federal Government for use in authenticating to facilities, networks, and systems.

A definition for a PIV-*Interoperable* credential for federal agencies is required to address:

- Identity assurance requirements,
- Authenticator assurance requirements,
- Technical interoperability clarifications,
- Security and auditing clarifications, and
- Procurement clarifications.

1.2 Scope

This document is limited to describing identity credentials that interoperate with the Federal Government PIV infrastructure and may be accepted by the Federal Government for access to data, applications, facilities, and networks.

This document does not address the use cases for when it is appropriate or allowed for federal agencies to directly issue alternate non-PIV credentials for interoperability with PIV to employees, contractors, and affiliates.

Version 2.0 of this document has been updated to:

- Remove many duplicative references to PIV-Interoperable requirements which have been stated in other government documents as authoritative,
- Update references and terminology, and
- Add clarification for federal departments and agencies on the scope of security, auditing, and procurement requirements.

1.3 Document Objectives

This document provides solutions for overcoming the barriers to federal reliance on identity credentials which are defined as interoperable with PIV. Four specific areas of concern have been identified:

1. **Common terminology for identity credentials and issuers** – To ensure consistency, a lexicon for differentiating a PIV credential from a credential interoperable with PIV infrastructure, and the differences between Non-Federal and Federal Issuers, has been developed.

2. **Assured identity** – The fundamental purpose of an identity credential is to establish the identity of the credential holder. Therefore, an identity credential must be issued in a federated model and consistent manner which provides the Federal Government with a requisite level of identity assurance.
3. **Technical requirements** – For identity credentials to be interoperable with the federal PIV infrastructure, basic technological requirements must be met.
4. **Security and auditing** – The boundaries for auditing and compliance requirements require clarification for federal agencies.

For each of these, a minimum set of requirements is described that will allow identity credentials to technically interoperate with Federal Government PIV systems and be trusted by Federal Government relying parties.

1.4 Assumptions

The following assumptions apply:

1. Federal departments and agencies determine the extent to which they will trust PIV-Interoperable credentials.
2. Possession of a PIV-Interoperable credential does not infer an access or authorization of any kind.
3. User privileges and entitlements (Authorization) are determined solely by the Federal Government relying party.
4. PIV-Interoperable credentials shall not be considered a substitute or alternative credential for populations otherwise subject to PIV requirements.

2 MINIMUM CREDENTIAL REQUIREMENTS

2.1 Common Terminology for Identity Credentials

To ensure consistency, a lexicon for differentiating a Federal Government PIV credential from a PIV-Interoperable credential was developed.

There is a lack of standard terminology to distinguish between characteristics of PIV credentials and PIV-Interoperable credentials in the identity credential space. This can result in confusion, uncertainty, or misunderstanding. This document resolves the terminology problem by proposing a more complete set of identity credential terms and scoping statements that unambiguously describe federal PIV credentials, federally issued PIV-Interoperable credentials, and non-Federally issued PIV-Interoperable credentials.

- **PIV credential** – An identity credential that is fully conformant with Federal Government PIV Standards including identity assurance, authenticator assurance, and baseline suitability assurance.
- **PIV-Interoperable credential** – An identity credential that is conformant with the Federal Government PIV Standards for identity assurance and authenticator assurance.

Table 1 provides a summary of the identity assurance, authenticator assurance, and baseline suitability assurance requirements.

Table 1: PIV and PIV-Interoperable Definitions

Assurance	Requirements Summary[2]	PIV	PIV-Interoperable
Identity Assurance: The robustness of the identity proofing process and the binding between an authenticator and a specific individual.	1. In-person proofing 2. Capture and verification of two (2) independent identity documents 3. Capture of biometrics	**Yes**	**Yes**

[2] Requirements are summarized only. For the detailed requirements, reference the source documents outlined in Section 2.2.

Assurance	Requirements Summary[2]	PIV	PIV-Interoperable
Authenticator Assurance: The robustness of the authentication process, and assurance that the user has possession of the authenticator.	1. Public key infrastructure key pairs 2. Biometric 3. Hardware based credential	**Yes**	**Yes**
Suitability Assurance: The investigative and adjudication processes which enhance the identity assurance. Suitability is associated with a position designation and/or risk assessment for determining an individual is suitable to work for or on behalf of the Federal Government.	● A minimum of: o A favorably adjudicated *National Agency Check with Inquiries*, or o A favorably adjudicated Tier 1 or higher federal background investigation.	**Yes**	**No**

All individuals issued PIV credentials are *required* to have common, minimum suitability assurance as specified in FIPS 201-2, Section 2.1 Control Objectives. Individuals with PIV-Interoperable credentials assert no suitability assurance in a baseline, standardized manner.

Section 2.2 outlines more information for the identity assurance, authenticator assurance, and suitability assurance.

2.2 Trusted Identity

The fundamental purpose of an identity credential is to establish a trust foundation based on:

- the *identity assurance* of the person, and
- the *authenticator assurance* of the credential.

Therefore, the PIV-Interoperable credentials must be issued in a manner that provides the Federal Government with a commensurate level of trust for *identity assurance* and *authenticator assurance*.

For PIV credentials, individuals are also required to have common, minimum suitability assurance defined as:

- a baseline suitability assurance of the person to work for or on behalf of the Federal Government.

Suitability assurance may not be determined from a PIV-Interoperable credential.

2.2.1 PIV-Interoperable Identity Assurance

The Federal Government's *identity assurance* requirements are defined in FIPS 201-2 for PIV credentials. The PIV-Interoperable credentials shall adhere to the same *identity assurance* requirements as PIV credentials. A summation of the *identity assurance* requirements is defined here for informational purposes only.

- In-person appearance and proofing
- Verification of two independent identity documents or accounts
- Capture of biometrics

The full list of requirements for identity assurance for PIV-Interoperable credentials is listed in the **X.509 Certificate Policy for the Federal Bridge Certification Authority.**

Table 2 identifies the PIV-Interoperable Level of Assurance *and* Identity Assurance levels as mapped to the Office of Management and Budget (OMB) Memorandums and National Institute of Standards and Technology (NIST) Special Publications.

Table 2: Identity Assurance of PIV-Interoperable Credentials

Level of Assurance[3]	Identity Assurance Level[4]
Level of Assurance 4	**Identity Assurance Level 3**

2.2.2 PIV-Interoperable Authenticator Assurance

The PKI certificates are where the identity assurance and authenticator assurance *are asserted* during use in networks, facilities, and systems. All PIV-Interoperable identity credentials must contain certificates issued from one of the Certification Authorities which operate under the Federal Public Key Infrastructure (Federal PKI) Certificate Policies.

There are two Certificate Policies which govern the Federal PKI Certification Authorities:

- Certificate Policy for the Federal Bridge Certification Authority
- Certificate Policy for the Federal PKI Common Policy Framework

There are Certification Authorities which operate and are audited for compliance to these Certificate Policies. The Certification Authorities also have Registration Authority services which may be built or operated by third-parties such as federal agencies or commercial service providers. The Registration Authority services encompass *the systems* and *processes* where the initial collection of the Personally Identifiable Information (PII) is performed for the PIV or PIV-Interoperable identity assurance and lifecycle management functions.[5] All Certification Authorities and Registration Authority components are subject to audits for compliance to management, operational, and technical controls specified in their respective Certificate Policies.[6]

Within this boundary of more than 100 existing and audited Certification Authorities, there are options operated and available for direct use by federal departments within the Executive Branch. There are also Certification Authorities which are operated for non-federal Executive

[3] As defined in OMB Memorandum 04-04 and NIST Special Publication 800-63-2.

[4] As defined in *draft* NIST Special Publication 800-63-3. The 800-63 Revision 3 (800-63-3) specifies three levels for identity assurance which are mapped to the four overall levels of assurance.

[5] This includes Card Management Systems and any associated software or hardware components used to collect and manage information used in the issuance and lifecycle management for PIV or PIV-Interoperable credentials.

[6] The compliance audits may include the Certificate Policies maintained by the Certification Authority which are mapped to the Certificate Policy for the Federal Bridge or the Certificate Policy for the Federal PKI Common Policy Framework.

Branch entities including Legislative and Judicial Branch agencies, and State, Local, Tribal, Territorial, International, and Commercial Partners.

The Certificate Policies extension object identifier (OID) contained in the certificates asserts the identity assurance of the person presenting the credential and certificate, how the private keys are stored and managed, and how the certificate should be validated for usage.

However, the Certificate Policies extension OID for the PIV Authentication Certificates is available only to Federal Government organizations. PIV-Interoperable authentication certificates may not assert the PIV Certificate Policies OIDs used for PIV Authentication. Therefore, additional policy defines comparable Certificate Policies' OIDs that can be trusted by the Federal Government for use in PIV-Interoperable Authentication Certificates.

The **X.509 Certificate Policy for the Federal Bridge Certification Authority** specifies the minimum requirements for the Federal Government to rely on PIV-Interoperable credentials, and includes all requirements for PIV-Interoperable credentials inclusive of:

- Certificate policy extension object identifiers,
- Clarification on identifier namespaces to be used, and
- Credential requirements for security and auditing.

All issuers of PIV-Interoperable credentials shall adhere to the requirements for PIV-Interoperable credentials outlined in the **X.509 Certificate Policy for the Federal Bridge Certification Authority**.

Operationally, the Certification Authorities and Registration Authorities that may be subordinate to the **Certificate Policy for the Federal PKI Common Policy Framework** must map their management, security, and operational controls for PIV-Interoperable credentials without needing a *cross-certificate* directly from the Federal Bridge Certification Authority. Policy mapping may be used; the Certification Authority must receive a certificate from Common Policy Framework which maps the Federal Bridge Certification Authority policy OIDs to the issuing Certification Authority's OIDs for PIV-Interoperable.

Table 3 identifies the PIV-Interoperable Authenticator Assurance levels as mapped to the Office of Management and Budget (OMB) Memorandums and NIST Special Publications.

Table 3: Authenticator Assurance of PIV-Interoperable Credentials

Level of Assurance[7]	Authenticator Assurance Level[8]
Level of Assurance 4	**Authenticator Assurance Level 3**

2.2.3 PIV-Interoperable Suitability Assurance

Suitability assurance is defined as the investigative and adjudication processes which *enhance* the identity assurance. These processes are used to determine suitability for granting access to federal data, applications, facilities, and networks. Only the Federal Government may determine the fitness or suitability of an individual for access to Federal Government assets.

PIV-Interoperable processes are unable to mirror the suitability assurance processes employed for the PIV credential. PIV-Interoperable credentials assert no suitability assurance in a *baseline, standardized manner*.

A Federal Government relying party may associate the PIV-Interoperable credential with additional off-credential information to determine the fitness or suitability of the requested access. Examples of off-credential information could be a record check against investigation databases, an entitlements attribute, or other manual or automated processes.

PIV-Interoperable credentials may be appropriate for situations where an agency has determined that a PIV credential is not warranted, but the individual requires access. Such situations may include, but are not limited to:

- Temporary/seasonal employees, visiting scientists and guest researchers, or contractor personnel requiring access for less than six (6) months;
- Non-U.S. nationals with insufficient residency in the U.S. to satisfactorily conduct the background investigation; and
- Personnel operating outside the contiguous U.S. under special risk security considerations, as outlined in FIPS 201-2.

A standardized set of procedures and processes for suitability assurance covering any or all of these possible use cases is outside the scope of this document.

[7] As defined in OMB Memorandum 04-04 and NIST Special Publication 800-63-2.

[8] As defined in NIST Special Publication 800-63-3. The 800-63 Revision 3 (800-63-3) specifies three levels for authenticator assurance which are mapped to the four overall levels of assurance.

Where suitability is a concern for a federal agency, the agency may require further suitability checks prior to granting any access. This document does not prohibit a suitability and fitness determination from being required by federal departments and agencies prior to issuing a federal PIV-Interoperable credential *or* granting any access to an individual with a PIV-Interoperable credential.

2.3 Federal Issuers and Non-Federal Issuers for PIV-Interoperable Credentials

For PIV-Interoperable credentials, there may be Federal Issuers and Non-Federal Issuers who participate. Many documents have asserted the term "Non-Federal Issuer" or NFI as synonymous with a PIV-Interoperable credential; the two terms are different and there is a need to clarify the terminology.

Two (2) sample scenarios are outlined in Table 4 to clarify the difference between a NFI and a Federal Issuer of PIV-Interoperable credentials.

Table 4: Scenarios of a Non-Federal and Federal Issuer of PIV-Interoperable Credentials

	Scenario A: Non-Federal Issuer	Scenario B: Federal Issuer
Description	Federal Agency **A** has affiliates or service providers who have persons who manage data systems, or need access to the federal networks or facilities	Federal Agency **B** has affiliates or persons who manage data systems, or need access to the federal networks or facilities
Scenario Outline	Federal Agency A: 1. Requests partners, affiliates, or service providers to have their contracted or employee personnel obtain PIV-I credentials 2. Provides the request through a Department or Agency-level Policy, Memorandum, or contract action with the affiliate or service provider 3. The partner, affiliates, or service provider chooses the PIV-I service or builds their own, and makes any contractual or other arrangements with the PIV-I service	Federal Agency B: 1. Selects a PIV-I credentialing service to use 2. Pays for or builds the PIV-I service 3. Authorizes and directs persons to use a designated PIV-I service and receive PIV-I credentials 4. Has responsibility for the sponsoring of persons, lifecycle management, and other activities including revoking the credentials after the person terminates any service

	Scenario A: Non-Federal Issuer	Scenario B: Federal Issuer
Type	*Non-Federal Issuer of PIV-Interoperable Credentials*	*Federal Issuer of PIV-Interoperable Credentials*
Examples	● State, Local, Tribal, and Territorial partners ● Aerospace and Defense partners ● Financial Services partners	● Federal Agency B has determined that persons under their authority require PIV-Interoperable credentials to meet a use case where PIV credentials do not apply

For these two scenarios:

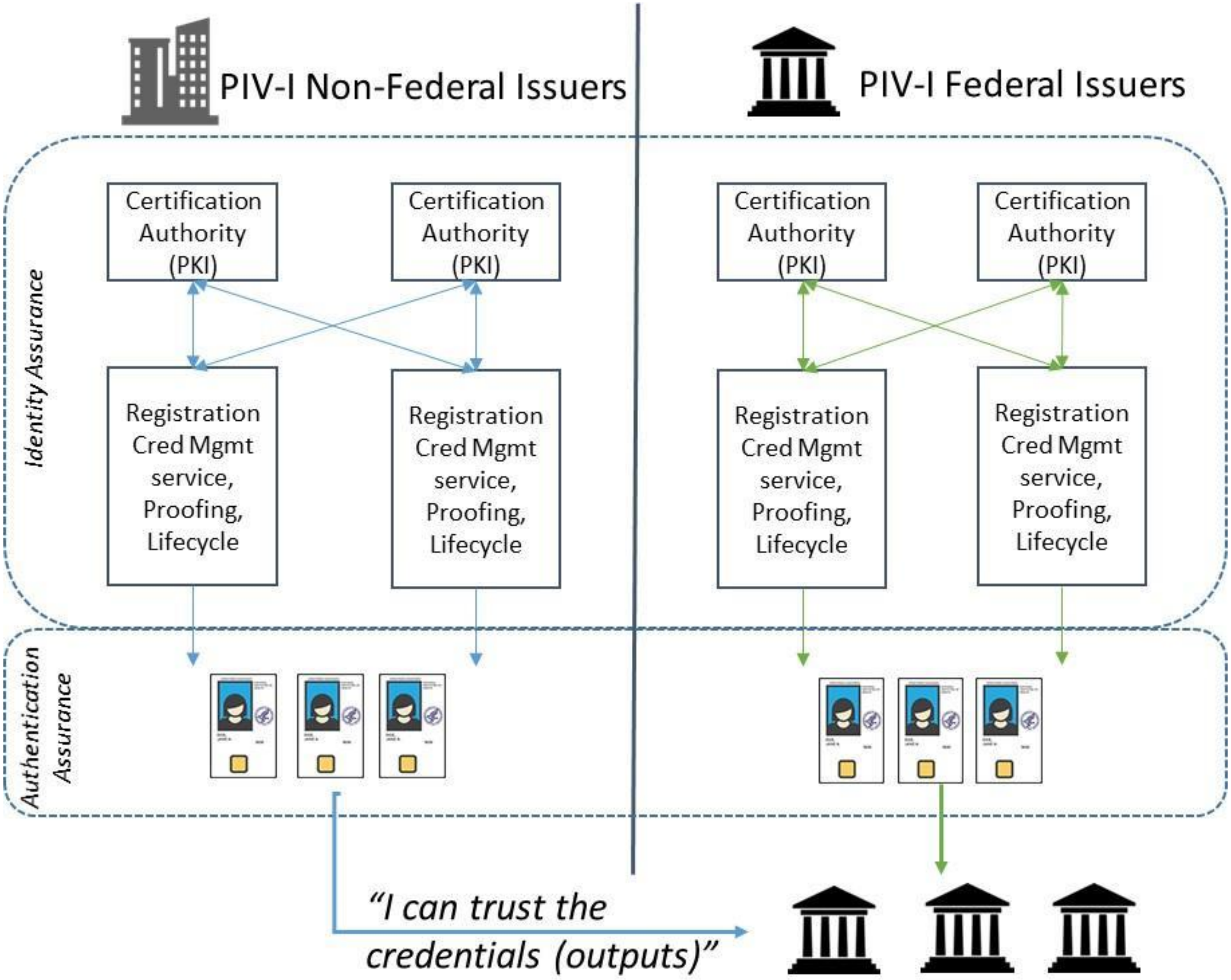
- Scenario A is a Non-Federal Issuer
- Scenario B is a Federal Issuer

Federal agencies may choose to trust and accept the NFI PIV-Interoperable credentials, and acceptance of NFI PIV-Interoperable credentials has financial and interoperability benefits for government-wide purposes.

Figure 1 outlines the identity assurance services and components, the authenticator assurance components, and the NFI versus Federal Issuer distinction. Figure 1 shows two (2) certification authorities and two (2) registration, credential management, identity proofing, and lifecycle service components for each scenario to illustrate that any one individual Certification Authority system may have more than one Registration Authority system, and vice versa.

Figure 1 is used in later sections of this document to identify the auditing and security requirements applied to each scenario.

Figure 1: Non-Federal Issuers and Federal Issuers for PIV-Interoperable Credentials[9]


PIV-I Non-Federal Issuers
PIV-I Federal Issuers
Identity Assurance
Certification Authority (PKI)
Certification Authority (PKI)
Certification Authority (PKI)
Certification Authority (PKI)
Registration Cred Mgmt service, Proofing, Lifecycle
Registration Cred Mgmt service, Proofing, Lifecycle
Registration Cred Mgmt service, Proofing, Lifecycle
Registration Cred Mgmt service, Proofing, Lifecycle
Authentication Assurance
"I can trust the credentials (outputs)"

2.4 Technical Requirements

Basic technology requirements must be met for identity credentials to interact with the Federal Government's infrastructure for PIV credentials. PIV-Interoperable credentials must conform to NIST technical specifications for PIV credentials, as defined in:

- **FIPS 201-2**
- **NIST Special Publication 800-73-4**
- **NIST Special Publication 800-78-4**
- **NIST Special Publication 800-76-2**

[9] No suitability assurance shown. PIV-Interoperable credentials when issued by either non-federal or federal entities assert no standardized suitability and fitness determinations.

Further clarification of the NIST Special Publications is required to address 1) visual distinction and 2) identifiers.

2.4.1 Visual Distinction

PIV-Interoperable credentials shall contain distinctive markings indicating the issuing entity and shall be visually distinct from PIV credentials. Common options for visual distinction include being printed in a horizontal (landscape) layout versus a vertical layout, or displaying PIV-I in one of the optional printed fields. The horizontal (landscape) layout is recommended to promote consistency in visual distinction.

2.4.2 Identifier Namespace

Effective use of PIV and PIV-Interoperable identity credentials requires one or more identifiers to support the interoperability and use in distributed systems across the Federal Government.

PIV credentials include a number of identifiers which can be used to link the credential to accounts in physical access control systems (PACS), networks, and applications. These identifiers include, but are not limited to:

- Card Universally Unique Identifier (Card UUID)
- Card Holder Unique Identifier (CHUID)
- Federal Agency Smart Credential Number (FASC-N)

PIV-Interoperable credentials have these same requirements for identifiers. While FIPS 201-2 deprecates the use of the CHUID *authentication* mechanism, the CHUID and FASC-N remain elements of the PIV Data Model and these elements may still be in use in legacy physical access control systems for account linking purposes.

There are additional challenges for PIV-Interoperable credentials. For example:

- The FASC-N number scheme is a smart number which incorporates a federal agency code.
- The FASC-N cannot be easily extended to allow sufficient identifier namespace to support PIV-Interoperable credentials issued by NFIs including State, Local, Tribal, Territorial, or Commercial Partners.
- The **X.509 Certificate Policy for Federal Bridge Certification Authority** does not specifically address Federal Issuers of PIV-Interoperable credentials and FASC-N numbering schema.

For these reasons, the FASC-N requires specific attention for PIV-Interoperable credentials.

Requirements for the FASC-N are:

- NFIs of PIV-Interoperable credentials are required to generate and issue FASC-N values which populate the value "9" for the Agency Code, System Code, and Credential Number:
    - This results in fourteen (14) nines: 9999 9999 999999

- Federal Issuers of PIV-Interoperable credentials are *strongly encouraged* to generate and issue FASC-N *values* that comply with the requirements for *NFIs* of PIV-Interoperable credential, including:
    - ○ Populating the fourteen (14) nines for the Agency Codes, System Codes, and Credential Number: 9999 9999 999999

- Federal Issuers of PIV-Interoperable credentials *may choose* to generate and issue FASC-N values which contain their assigned Agency Codes[10], System Codes, and a Credential Number, in accordance with their PIV Card Issuer Authorization[11]

- Federal Issuers of PIV-Interoperable credentials who choose to generate and issue FASC-N values which contain their assigned Agency Codes, a System Code, and a Credential Number, shall be aware that:
    - ○ Provisioning and use of the federally issued PIV-Interoperable credentials in facility access may be negatively impacted

Table 5 outlines the different scenarios for issuers of PIV-Interoperable credentials, the portion of the FASC-N values impacted, and issues expected to be encountered and mitigated.

[10] NIST Special Publication 800-87

[11] NIST Special Publication 800-79-2

Table 5: FASC-N Values for PIV-Interoperable Credentials and Issues

Issuer of PIV-Interoperable	FASC-N Value	Issues
Non-Federal	Agency Code, System Code, and Credential Number must be all “9”s 9999 9999 999999	Departments and agencies with PACS which solely use FASC-N for account linking should not use PIV-Interoperable credentials for unattended facilities access. The PACS should be updated to use the Card UUID value for the account linking.
Federal	Agency Code, System Code, and Credential Number strongly encouraged to be all “9”s 9999 9999 999999	Departments and agencies with PACS that solely use FASC-N for account linking should not use PIV-Interoperable credentials for unattended facilities access. The PACS should be updated to use the Card UUID value for the account linking.
Federal	Agency Code, System Code, and Credential Number may be populated 1300 0002 456859	PACS that use the presence of the “9” values to determine whether the credential is a PIV-Interoperable or PIV credential may reject the federally issued PIV-Interoperable credential during use. The PACS may be erroneously checking that the FASC-N is populated with non-“9” values and attempting to validate a PIV certificate extension policy OID instead of the PIV-Interoperable certificate extension policy identifier. The PACS should be updated to use the Card UUID value for the account linking.

3 Special Considerations for Federal Agencies

Federal agencies have identified the need to clarify the differences between:

- the auditing performed to maintain compliance with the Federal PKI,
- the auditing performed and required for PIV or PIV-Interoperable credential issuers to be granted an authorization to operate under the NIST Special Publication 800-79,
- the Federal Information Security Modernization Act (FISMA) Authorization to Operate, and
- contracting or procurement requirements.

This section helps clarify these differences and the boundaries for federal agency Chief Information Security Officers.

3.1 Auditing Requirements

There are four primary documents referenced for security controls and audit requirements for the systems used for issuing either PIV or PIV-Interoperable credentials:

1. **NIST Special Publication 800-53** identifies the security control categories to be used for all systems
2. Federal PKI defines the **Security Controls Overlay of Special Publication 800-53 Security Controls for PKI Systems**
3. **NIST Special Publication 800-79-2** identifies operational audits for the PIV credentialing activities
4. Federal PKI defines the **FPKI Compliance Audit Requirements**

For auditing, the Federal PKI requires:

- Certification Authorities to be *audited*
- Any Registration Authority systems and processes which are used by the Certification Authority to issue PIV or PIV-Interoperable credentials to be *audited*
- Audits must encompass:
    - the Security Controls Overlay of **NIST Special Publication 800-53**,
    - the applicable **NIST Special Publication 800-79-2** requirements, and
    - the compliance with the Certification Authority's Certificate Policy and Certification Practices Statements.

The audits are performed by third-party independent auditors and audit results must be submitted to the Federal PKI on a recurring basis. In addition to the third-party independent audits, the Certification Authorities and Registration Authority systems must submit to the Federal PKI on a recurring basis:

- Samples of outputs from the systems for compliance inspection and testing, including:
  - Samples of all Certificate types issued, and
  - Samples of any PIV or PIV-Interoperable credentials issued.

These sample artifacts are used to perform compliance inspection on the *outputs* of the systems in addition to the management, operational, and technical controls which are inspected during the audits. Non-compliant sample artifacts are reported to the Certification Authority, Registration Authority, or federal agency and remediation of non-compliant elements must be addressed or the entities will lose their compliance certification.

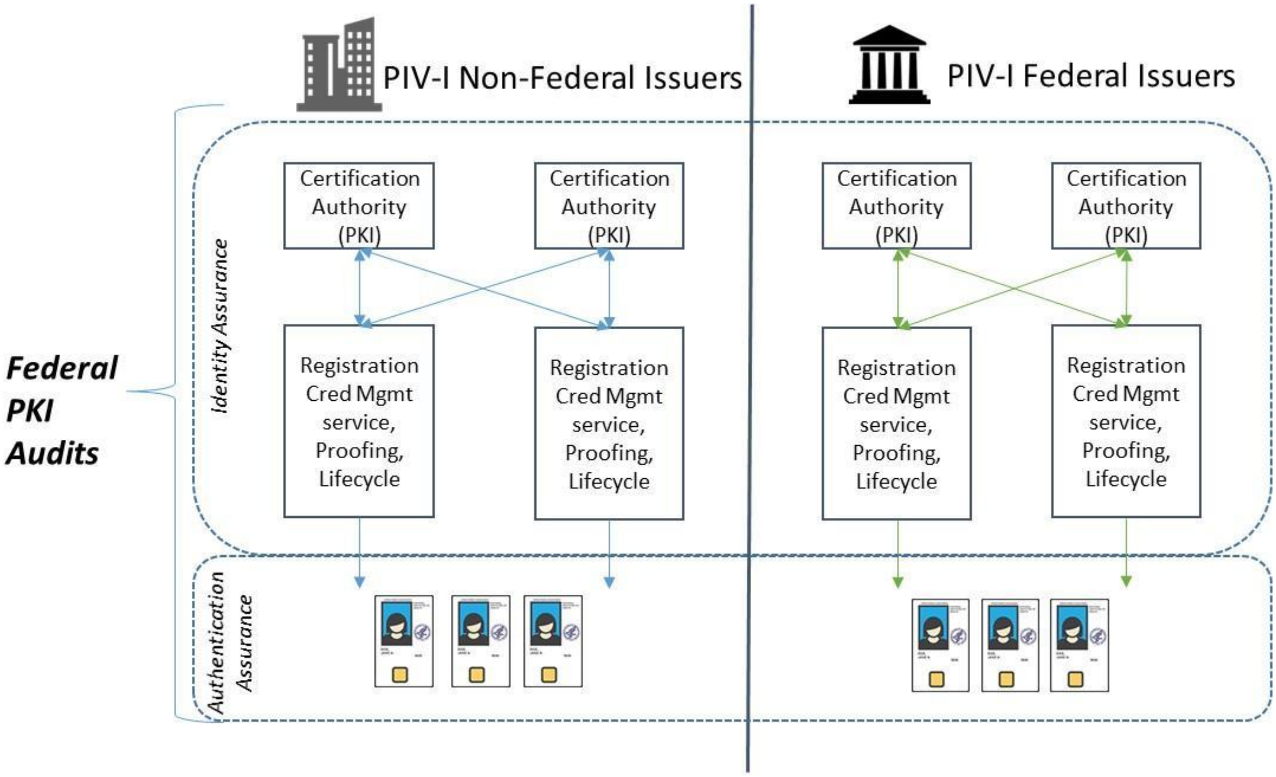
The audits and the compliance or non-compliance of the Certification Authority or Registration Authority components are used by the Federal Government, other public sector, international, or commercial entities to assert a number of claims on websites, product documentation materials, memorandums, or contracting documents. These claims often include:

- Federal PKI Provider
- PIV Provider
- PIV-Interoperable Provider
- Compliance with the Federal PKI

When asserting these claims, the audits and the associated processes and procedures are establishing the capability for federal agencies to trust the outputs of the systems and the credentials issued from the systems.

Figure 2 shows the boundaries of the Federal PKI audit and compliance activities.

Figure 2: PIV-Interoperable Credentials and Federal Public Key Infrastructure Audit Boundaries


PIV-I Non-Federal Issuers
PIV-I Federal Issuers
Federal PKI Audits
Identity Assurance
Authentication Assurance
Certification Authority (PKI)
Certification Authority (PKI)
Certification Authority (PKI)
Certification Authority (PKI)
Registration Cred Mgmt service, Proofing, Lifecycle
Registration Cred Mgmt service, Proofing, Lifecycle
Registration Cred Mgmt service, Proofing, Lifecycle
Registration Cred Mgmt service, Proofing, Lifecycle

A FISMA Authorization to Operate is a separate and distinct assertion. The Federal PKI audits and processes do not assert that there is a Federal Government Designated Authorizing Official or *continuous monitoring* requirements in place for *all* Certification Authorities or Registration Authority components.

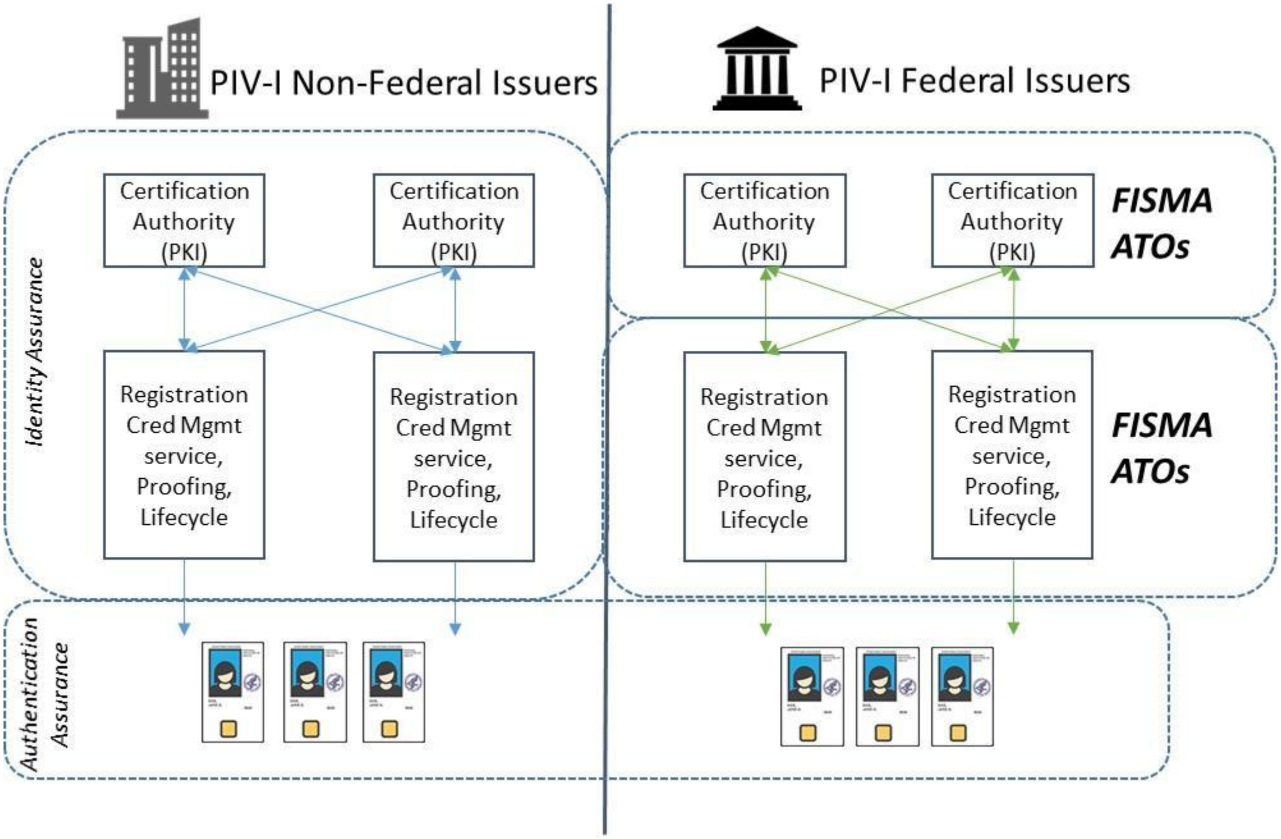
Although the PIV-Interoperable issuers for non-federal entities may be operated and have continuous monitoring that are commensurate with commercial best practices, the federal agencies are still required to assume responsibility for any government data placed into systems which are bought, built, or used.

Prior to *directly placing* any PII in a service used to issue and manage PIV-Interoperable credentials or procuring any such service, federal agencies are required to confirm and request:

- Audit Compliance Letters for Federal PKI compliance
- An ATO Memorandum signed by a Federal Government Designated Authorizing Official (DAO)
- Confirmation of compliance with continuous monitoring requirements

Figure 3 shows the notional system boundaries of the required FISMA ATO for Federal agencies and issuers of PIV-Interoperable credentials.

Figure 3: PIV-Interoperable Credentials and FISMA ATO


PIV-I Non-Federal Issuers
PIV-I Federal Issuers
Identity Assurance
Certification Authority (PKI)
Certification Authority (PKI)
Certification Authority (PKI)
Certification Authority (PKI)
FISMA ATOs
Registration Cred Mgmt service, Proofing, Lifecycle
Registration Cred Mgmt service, Proofing, Lifecycle
Registration Cred Mgmt service, Proofing, Lifecycle
Registration Cred Mgmt service, Proofing, Lifecycle
FISMA ATOs
Authentication Assurance

In addition, federal agencies using PIV-Interoperable services must request from the provider the Registration Authority Agreement. The Registration Authority Agreement must explain how the provider has implemented the credential management and lifecycle management requirements of the PIV-Interoperable Certificate Policy. The contents of the Registration Authority Agreement must be approved by the PIV-Interoperable provider’s policy authority as satisfactorily implementing the requirements, and submitted to the Federal PKI as part of the audit artifacts.

Table 4 summarizes the FKI auditing and FISMA *Authority to Operate* distinctions.

Table 4: Federal Public Key Infrastructure Auditing and FISMA ATO Comparison

	Scenario A: Non-Federal Issuer	Scenario B: Federal Issuer
Type	Non-Federal Issuer of PIV-Interoperable Credentials	Federal Issuer of PIV-Interoperable Credentials
Federal PKI Audits	1. Annual Audits for the Certification Authorities directly 2. Annual Audits of the services and systems used with the Certification Authorities to collect information and manage credentials 3. Submission of sample artifacts for compliance testing	1. Annual Audits for the Certification Authorities directly 2. Annual Audits of the services and systems used with the Certification Authorities to collect information and manage credentials 3. Submission of sample artifacts for compliance testing 4. Applicable **NIST Special Publication 800-79-2** requirements
FISMA Authorization to Operate		● Additional security controls ● Continuous monitoring ● Government Designated Authorizing Official
Items to be Requested or Produced	1. Audit Compliance Letters for Certification Authorities 2. Audit Compliance Letters for Registration Authority components (inclusive of any Card Management systems)	1. Audit Compliance Letters for Certification Authorities 2. Audit Compliance Letters for Registration Authority components (inclusive of any Card Management systems) 3. Authorization Memorandum issued by and signed by the Government Designated Authorizing Official 4. Registration Authority Agreements

3.2 Acquiring PIV-Interoperable Services

When contracting either through interagency agreements or commercially sourced services for PIV-Interoperable services, federal agencies may have several choices concerning the extent of the service. As a federally-contracted service storing PII of persons under the authority of the federal agency, all contracts and procurement language must include the requirements to:

- Have an existing FISMA Authorization to Operate or provisions to obtain and maintain an Authorization to Operate
- Submit to continuous monitoring, inclusive of requirements for penetration testing and vulnerability scanning by the Federal Government

This must be a condition of the contract, and contract language should make it clear that failure to comply with FISMA and other security requirements will result in summary termination of the contract.

A further consideration is the System of Records Notice (SORN). Many agencies should, wherever possible, be able to leverage the SORN associated with the issuance of PIV credentials for the issuance of PIV-Interoperable credentials, since the purpose of PIV-Interoperable issuance is within its scope.

APPENDIX A: TECHNICAL INFORMATION

This Appendix provides additional technical information in support of the technical requirements. The following table provides a comparison of the requirements for each credential type.

	Technical Requirements	PIV	PIV-Interoperable
Trust	Identity Assurance ● Level of Assurance 4 ● Identity Assurance Level 3 (draft NIST SP 800-63-3)	●	●
	Authenticator Assurance ● Level of Assurance 4 ● Authenticator Assurance Level 3 (draft NIST SP 800-63-3)	●	●
	Suitability Assurance: ● Favorably adjudicated National Agency Check with Inquiries (minimum) or other Tier 1 investigation	●	
	PIV policy object identifier on PIV Authentication Certificates	●	
	PIV-I equivalent policy object identifier on PIV-I Authentication Certificates		●
	PIV Content Signing object signing certificate	●	
	PIV-I Content Signing equivalent object signing certificate		●
	Card stock certified	●	●
	PIV Application Identifier (AID)	●	●
	Command edge and NIST SP 800-85 conformant	●	●

	Technical Requirements	PIV	PIV-Interoperable
Credential Edge	NIST SP 800-73-4 conformant GUID present in the CHUID	●	●
	RFC 4122 conformant UUID required in the GUID data element of the CHUID	●	●
	RFC 4122 conformant UUID present in the Authentication Certificates	●	●

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.
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.
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 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.
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 credential reader) and may involve human control (e.g., a security guard).
PIV-Interoperable credential	An identity credential that is conformant with the federal PIV Standards for identity assurance and authentication assurance

Term	Definition
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.

APPENDIX C: ACRONYMS

Acronym	Definition
CA	Certification Authority
CP	Certificate Policy
CHUID	Card Holder Unique Identifier
FASC-N	Federal Agency Smart Credential - Number
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
GSA	General Services Administration
GUID	Global Unique Identification Number
HSPD-12	Homeland Security Presidential Directive 12
LACS	Logical Access Control System
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries
NFI	Non-Federal Issuer
NIST	National Institute of Standards and Technology
OID	Object Identifier
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PACS	Physical Access Control System
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	PIV-Interoperable

PKI	Public Key Infrastructure
SP	Special Publication
U.S.	United States
UUID	Universally Unique Identifier

APPENDIX D: DOCUMENT REFERENCES

FIPS 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors
http://csrc.nist.gov/publications/PubsFIPS.html

HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors
http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

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

NIST SP 800-63-2: Electronic Authentication Guideline
http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-63-3: Digital Identity Guidelines
http://csrc.nist.gov/publications/PubsSPs.html

NIST SP 800-73-4: 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 800-79-2: Guidelines for the Authorization of Personal Identity (PIV) Verification Card Issuers (PCI's) and Derived PIV Credential Issuers (DPCI)
http://csrc.nist.gov/publications/PubsSPs.html

OMB A-130: Management of Federal Information Resources
https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework
https://www.idmanagement.gov/fpki

X.509 Certificate Policy for the Federal Bridge Certification Authority
https://www.idmanagement.gov/fpki