NIST Special Publication 800
NIST SP 800-217 fpd

Guidelines for Personal Identity Verification (PIV) Federation

Final Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Justin P. Richer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-217.fpd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-217 fpd

Guidelines for Personal Identity Verification (PIV) Federation

Final Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Justin P. Richer
Bespoke Engineering

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-217.fpd

November 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [will be added upon final publication]

How to Cite this NIST Technical Series Publication

Ferraiolo H, Regenscheid A, Richer JP (2024) Guidelines for Personal Identity Verification (PIV) Federation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-217 fpd. https://doi.org/10.6028/NIST.SP.800-217.fpd

Author ORCID iDs

Hildegard Ferraiolo: 0000-0002-7719-5999
Andrew Regenscheid: 0000-0002-3930-527X
Justin P. Richer: 0000-0003-2130-5180

Public Comment Period

November 14, 2024 - January 10, 2025

Submit Comments

mailto:piv_comments@nist.gov

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/217/fpd, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

FIPS 201 defines the requirements and characteristics of government-wide interoperable identity credentials used by federal employees and contractors. It also calls for the federated use of those credentials. These guidelines provide technical requirements for federal agencies implementing digital identity services for federal employees and contractors and are not intended to constrain the development or use of standards outside of this purpose. This document focuses on the use of federated PIV identity and the use of assertions to implement PIV federations backed by PIV identity accounts and PIV credentials. Federation allows a PIV identity account to be used by relying parties outside the PIV identity account's home agency.

Keywords

assertions; authentication; credential service provider; digital authentication; electronic authentication; electronic credentials; federations; PIV credentials; PIV federation; identity providers; relying parties.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: mailto:piv_comments@nist.gov.

Table of Contents

List of Tables

List of Figures

1. Introduction

This section is informative.

PIV Cards and derived PIV credentials allow for a very high level of trust in a PIV identity account because of the requirements and processes used in the issuance of the PIV identity account, the features of the associated PIV Card, and the binding of derived PIV credentials to the PIV identity account. This document seeks to make the benefits of the PIV identity account available to federated relying parties (RPs) through the use of identity providers (IdPs) that verify PIV credentials and provide federated assertions representing the PIV identity account. Federation technologies can facilitate the connection of these PIV identity accounts across different security domains, allowing a subscriber to leverage the trust and strength of their PIV identity account at agencies other than the agency that issued the credentials.

1.1. Background

This document is a companion document to [FIPS201], providing specific details for implementing PIV federation for PIV identity accounts. [FIPS201] defines standards for the use of PIV credentials, including the establishment of the PIV identity account, the issuance of the PIV Card, authentication using the PIV Card, management of derived PIV credentials, and other aspects of the PIV identity account. FIPS 201 provides basic requirements for the use of federation and defers to the guidelines provided in this publication to define details of what a PIV-based federation system would entail.

[SP800-63C] and its companion document suite of [SP800-63] provide general guidelines for the use of federation technologies and assertions within Federal Government use cases. These guidelines are intended to be used across a wide variety of account types, authenticators, and deployment patterns. The SP 800-63 suite is not specific to PIV identity accounts.

This document, SP 800-217, specifically applies the guidelines of [SP800-63C] to the PIV identity account defined in [FIPS201] to outline the details of *PIV federation*. This document provides a set of processes and technical guidelines for deployers of PIV federation with Federal Government use cases in both IdP and RP roles.

1.2. Purpose and Scope

This document focuses on the use of federation technologies with PIV identity accounts for federal employees and contractors. This document does not discuss citizen-facing use cases covered in [SP800-63C]. This document does not address creation or life cycle of PIV identity accounts as covered in [FIPS201], nor does this document account for the issuance and management of derived PIV credentials in PIV identity accounts as covered in [SP800-157]. While the guidelines within this document could be generally useful in other circumstances, application to any additional use cases are outside the scope of this document.

1.2.1. Creating Technical Interoperability Profiles of This Guideline

The guidelines in this document alone are not intended to provide full technical interoperability profiles. In addition to this document and its prerequisites ([FIPS201], [SP800-63C], and [SP800-157]), PIV federation deployments will need technical interoperability profiles that are suitable for the federation protocol being used. The details of such profiles are out of scope for this document, but all technical interoperability profiles will need to consider the following points.

Target Protocols:

Different federation protocols can be used to fulfill the requirements in the guidelines of this document in different and often incompatible ways. A technical interoperability profile ought to target each specific federation protocol in order to allow for more stringent definitions.

Attribute Naming:

Each attribute that occurs within an assertion or the response from an identity API will need to have a name (or other means of address) defined. To ease interoperability, this name ought to reflect the value being asserted, such as `exp` for an expiration timestamp or `sub` for the subject identifier. Each entity of the federation has to use the same naming convention for interoperable attributes.

Attribute Contents:

Each attribute that occurs within an assertion or the response from an identity API will need to have its type, format, structure, or other content restrictions sufficiently defined such that the value can be unambiguously understood between sender and receiver. For example, a timestamp format could be encoded as an integer number of seconds since the UNIX Epoch GMT or in an ISO 8601 date string.

Conformance Criteria:

As PIV federation systems are likely to be built on top of existing federation software, a technical interoperability profile will need to define what additional options are allowed or forbidden by conformant implementations. For example, a profile of OpenID Connect could restrict use of the Implicit Grant Type for requests and responses.

Home Agency IdP Records:

Agencies need to have a means of publishing verifiable home agency IdP records in a known location that is easily reached and machine-readable by other parties. This could take the form of a centralized directory service with a query function or a lookup pattern based on domain names.

All technical interoperability profiles also need to consider existing profiles and industry best practices for the target technology in question.

1.3. Federation Use Cases

In a *direct authentication*, the claimant presents their authenticator to a verifier, which is tightly coupled with the RP and, usually, the home agency IdMS described in Sec 2.1.2. The verifier conducts an authentication process of a PIV credential. This process sometimes uses an external service, such as when public key infrastructure is used to validate a certificate.

PIV credentials are intended for use with direct authentication via the mechanisms listed in [FIPS201] and [SP800-157]. However, there are many situations in which direct authentication is not viable or desirable.

For example, non-PKI-based derived PIV credentials are bound and validated at the home agency. Federation allows these credentials to be used for accessing systems outside of the home agency by having the subscriber present the derived credential to the IdP, which can validate the credential and assert to the RP that the validation has taken place.

In a *federated authentication*, the verifier is not tightly associated with RP and is instead operated by a separate but trusted entity, the IdP. The PIV Card or derived PIV credential is used to authenticate the PIV cardholder to the IdP of a federation system. The IdP creates an *assertion* that represents the authentication event of the subscriber. The IdP sends this assertion to the RP using a federation protocol, and the RP verifies the assertion upon receipt.

In order to authenticate the subscriber, the IdP needs to perform the role of verifier for one or more PIV credentials in the PIV identity account. In some cases, the IdP is a service directly tied to the home agency IdMS. This tight coupling allows the IdP a direct view of the status of the PIV identity account and all associated PIV credentials. However, there are several mechanisms for a PIV IdP to be run by a party other than the home agency. For example, the home agency could outsource the IdP functionality and synchronize the state of its PIV identity accounts using a provisioning protocol or similar system. Alternatively, PKI-based PIV credentials can be verified by an IdP that is run by a party other than the home agency. In this scenario, the validity of the PIV identity account is inferred from the validity of the credential presented to the third-party IdP, and there is no connection to the home agency IdMS.

1.3.1. Federation Considerations

The use of a federation protocol allows RPs to be shielded from the complexities and requirements of managing individual authenticators. When a new authentication technology is adopted, only the IdP needs to be updated in order for the entire network to benefit. The home agency has the option to bind and manage any number of valid PIV credentials to the PIV identity account. The lifecycle of adding and removing authenticators to the PIV identity account does not affect the RP, which implements only the federation protocol.

Federation allows an RP to access PIV identity accounts that originate from different agencies on different networks. This connection allows an agency to leverage the identity infrastructure of another agency without needing to replicate the PIV identity account management process. The federation process allows the cardholder to use their established PIV credentials to authenticate to a variety of services through the PIV IdP without having to establish separate credentials at those RPs.

The subject identifier asserted by the IdP to the RP is stable to the PIV identity account over time and across different authenticators, including different certificates and attribute changes such as email address or name changes. The subject identifier can also be generated in a pairwise fashion for use cases that require a higher degree of privacy between multiple RPs while still providing a smooth user experience for the subscriber.

Many RPs need access to attributes about the subscriber, such as a display name or contact information. The fixed set of attributes included in a PIV certificate are presented as a whole to all RPs at which the certificate is presented, and some derived PIV credentials carry no attributes at all. In contrast, the attributes released during a federation transaction can vary depending on a variety of factors, including the nature of access required and the parameters of the RP. These attributes can include information in the PIV identity account that is not carried in any specific authenticator. In fact, these attributes are made available to the RP separate from the subscriber’s use of any particular authenticator.

An RP may want to verify that the PIV identity account is still active and has not been terminated, but in many circumstances, the RP will not have direct access to the PIV identity account. With federated protocols, the IdP is the authority for the accounts it asserts, allowing RPs to trust that these accounts are in good and current standing according to the IdP. When a PIV identity account is terminated, that account cannot be used to authenticate to the IdP and therefore can no longer be used at any connected RPs.

In advanced circumstances, the IdP and RP can engage in shared signaling about security events concerning accounts, agencies, and applications. These signals can inform a party about suspicious behavior with a given account or proactively indicate significant changes in an account’s status, such as termination, without the need for action on the subscriber’s part.

The RPs in a federation relationship transitively benefit from the security practices of the IdP. Instead of relying on all RPs to manage authenticators and accounts for many users over time, the IdP can act as a dedicated identity management device within the network.

This also means that an IdP would be aware of the usage of a given PIV identity account under its control at different RPs within its trust networks. While this has positive benefits for security, it does pose a privacy tradeoff wherein the IdP needs to be trusted with this usage information.

1.4. Audience

This document is intended for stakeholders who are responsible for procuring, designing, implementing, and managing deployments of PIV federation in both the IdP and RP roles.

1.5. Notations

This guideline uses the following typographical conventions in text:

- Specific terms in **CAPITALS** represent normative requirements. When these same terms are not in **CAPITALS**, the term does not represent a normative requirement.
    - The terms “ **SHALL** ” and “ **SHALL NOT** ” indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted.
    - The terms “ **SHOULD** ” and “ **SHOULD NOT** ” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.
    - The terms “ **MAY** ” and “ **NEED NOT** ” indicate a course of action permissible within the limits of the publication.
    - The terms “ **CAN** ” and “ **CANNOT** ” indicate a possibility and capability—whether material, physical, or causal—or, in the negative, the absence of that possibility or capability.

1.6. Document Structure

This document is organized as follows. Each section is labeled as either normative (i.e., mandatory for compliance) or informative (i.e., not mandatory).

- Section 2 describes a general architecture for PIV federation. This section is *informative*.
- Section 3 describes the trust agreements in a PIV federation. This section is *normative*.
- Section 4 describes the Federation Assurance Levels as applied to PIV federation. This section is *normative*.
- Section 5 describes the requirements for IdPs and RPs in a PIV federation. This section is *normative*.
- Section 6 describes the requirements for protocol elements in a PIV federation, including assertion contents. This section is *normative*.

- References contains a list of publications referred to from this document. This section is *informative*.
- Appendix A contains a glossary of selected terms used in this document. This appendix is *informative*.
- Appendix B contains a selected list of abbreviations used in this document. This appendix is *informative*.

2. Architecture

This section is informative.

PIV federation is the process by which a subscriber uses their PIV identity account to access an RP using an IdP for that account. As shown in Figure 1, the subscriber uses their PIV credentials (either a PIV Card or a derived PIV credential) to authenticate to the IdP and access the PIV identity account. The authentication event is then conveyed to the RP using an assertion that contains a set of attributes about the authentication event and the PIV identity account.

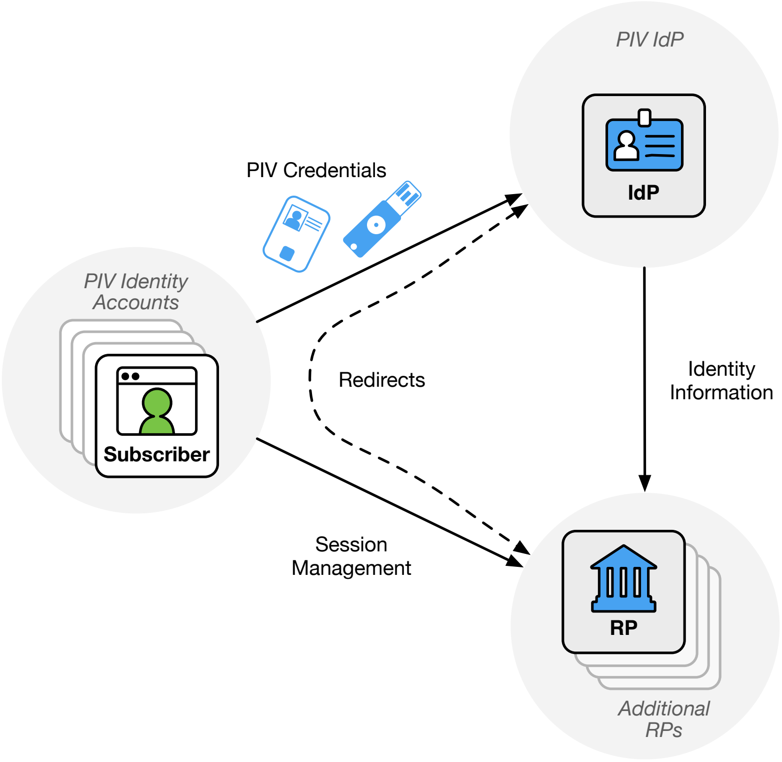

Fig. 1. PIV Federation

For PIV federation to occur, all of the following conditions apply:

- The account being asserted is a valid and active PIV identity account (see Sec. 2.1).
- The RP has established the IdP as the PIV IdP for the account through a valid and current trust agreement (see Sec. 2.2.1).
- The subscriber authenticates to the IdP using a PIV credential (see Sec. 2.1.1) or has provisioned the subscriber-controlled wallet by authenticating with a PIV credential (see Sec 2.2.3).

If any of these items are not true, such as the use of a non-PIV identity account at a PIV-enabled IdP or the authentication of a PIV identity account through an IdP that is not the PIV IdP for the account, then the transaction does not meet the requirements of PIV federation, and therefore the definitions and requirements in this document do not apply.

A successful PIV federation transaction is, roughly, as follows:

1. The subscriber starts in an unauthenticated state at the RP.
2. The RP requests a federated login at the IdP.
3. The subscriber authenticates to the IdP using a PIV credential (i.e., a PIV Card or derived PIV credential).
4. The IdP generates an assertion that represents the subscriber's PIV identity account to the RP.
5. The RP receives the assertion and processes it.
6. The RP creates an authenticated session for the subscriber. At the establishment of this session, the subscriber is logged in to the RP.

2.1. PIV Identity Account

A PIV identity account, as established in [FIPS201], is the digital account of a PIV cardholder, a party also known as the subject or subscriber in [SP800-63]. This account contains a set of identity attributes for the subscriber, bindings to all PIV credentials for the account, metadata about the account's creation, and identification of the home agency for the account.

The PIV identity account is the definitive source of PIV cardholder information in the context of PIV federation transactions, whether this information is communicated directly from that source to an RP (see *home agency IdP* in Sec. 2.2.2) or from another entity trusted by an RP to have accurate and timely information aligned with the PIV identity account records (see *PIV IdP* in Sec. 2.2.1). The strong identity proofing used in establishing this account, along with the processes used to manage the attributes and authenticators bound to this account, provide the foundation for trust in PIV identity assertions.

While the systems involved in PIV federation may also manage non-PIV accounts, the use of these accounts is outside the scope of this specification.

2.1.1. PIV Credentials

Authentication to a PIV identity account is accomplished using one or more PIV credentials that are bound to the account. PIV credentials can take the form of different kinds of authenticators that are each suitable for different purposes and use cases. The primary credential for a PIV identity account is the PIV Card, which is issued to the subscriber, as defined in [FIPS201]. A PIV identity account can also have multiple derived PIV credentials bound to it, as described in [SP800-157]. For the purposes of PIV federation, the PIV credential is presented to the PIV IdP to authenticate the cardholder to the PIV IdP.

2.1.2. Home Agency Identity Management System

The canonical record for a PIV identity account is stored in the identity management system (IdMS) of the home agency of the PIV identity account, known in this document as the home agency IdMS. This system stores and manages the attributes, statuses, and set of PIV credentials that are bound to the PIV identity account. In the terms of [SP800-63], the PIV identity account is the subscriber account, and the CSP acts on behalf of the home agency to establish the PIV identity account.

Some systems can have a direct view into the current state of a PIV identity account at the home agency IdMS, such as through a provisioning API at a federated RP. Such systems allow for a proactive propagation of information from the authoritative source, informing downstream systems of account changes as they happen.

Other systems have an indirect view of the status of the PIV identity account, such as by checking the status of the authentication certificate from a PIV Card. If the certificate is not revoked, it can be assumed that the PIV identity account it represents is still valid. However, the inverse is not true, as a revoked certificate could have been replaced for a still-valid PIV identity account during its normal lifecycle process.

In both of these systems, information from the home agency IdMS to the other systems may bye delayed or interrupted. For example, the certificates from a PIV Card can be revoked hours after the PIV identity account has been terminated. Even after the revocation occurs, the processes for updating the certificate revocation list or OCSP status listing are susceptible to latency as that information traverses the certificate issuer and validation systems. While such systems are designed to reach eventual consistency, the potential delays and failures need to be accounted for when designing a system.

2.2. Identity Providers

As described in [SP800-63C], the IdP provides a bridge between the PIV identity account (established in the home agency IdMS) and the RP using a federation protocol. In a federation transaction, the IdP acts as the verifier for the authenticator held by the subscriber. In the case of PIV federation, this means that the IdP verifies the PIV credential bound to the PIV identity account, as discussed in Sec. 2.1.1.

The IdP sends a cryptographically verifiable message called an *assertion* to the RP that identifies the PIV identity account being authenticated. The assertion contains attributes associated with that PIV identity account and details about the authentication event, as discussed in Sec. 6.2. The IdP can also make PIV identity account attributes available through a protected identity API alongside the assertion, as discussed in Sec. 6.5.

A *PIV IdP* is the IdP trusted by an RP to issue assertions for a given PIV identity account. From the perspective of the RP, all PIV federation transactions involve a PIV IdP. A PIV IdP is trusted by the RP to issue accurate and timely assertions regarding a PIV identity account. The means by which the PIV IdP obtains this information is outside of the scope of these guidelines, but many IdMSs integrate with federation services to provide an IdP capability. When the PIV IdP is not directly integrated, the account status can be ascertained by other means, such as querying the PIV identity account issuer through an API or inferring the account status from the status of the PKI-based PIV credential used to authenticate to the PIV IdP.

The *home agency IdP* (see Sec. 2.2.2) is the officially designated PIV IdP established by the home agency, which is the agency employing a federal employee or contractor. As a consequence, the home agency IdP is expected to have a direct view of the PIV identity account and PIV credentials associated with the account, including PKI-based and non-PKI-based authenticators. Because there may be multiple PIV IdPs capable of issuing assertions for a PIV cardholder, each home agency will need to identify the home agency IdP for the cardholders they serve, as discussed in Sec 3.5. The designation and use of a home agency IdP is required for all transactions at FAL2 and above.

The Federation Assurance Level (FAL) of a federation transaction places requirements on the parties of the transaction, as defined in [SP800-63C]. At FAL2 and FAL3, the PIV IdP trusted by the RP has to be the home agency IdP for the PIV identity account in question, as discussed in Sec. 4. Additional requirements for the home agency IdP are discussed in Sec. 3.5. At FAL1, the IdP could be operated or controlled by an entity other than the agency responsible for the PIV identity account. Some forms of PIV credential (such as PKI-based authenticators) can support such third-party operation of an IdP by allowing the authenticator to be verified across domains, which enables a PIV IdP to exist apart from the home agency's identity management systems.

2.2.1. PIV IdP

The PIV IdP is the PIV IdP identified in a trust agreement to provide federated assertions for a population of PIV identity accounts for an RP. Establishment of the PIV IdP in the trust agreement is discussed in greater detail in Sec. 3.

The population of PIV identity accounts served by a given PIV IdP can be determined based on a variety of factors but is usually based on the home agency of the PIV identity account. That is to say, an trust agreement will indicate that an agency's PIV identity accounts will be served by one specific IdP. Within any trust agreement, the RP needs to know which IdP to accept assertions about a particular PIV identity account from.

Different trust agreements can indicate different PIV IdPs for the same population of PIV identity accounts. For example, one RP could point to an integration service that acts as a proxy, while a different RP could connect directly to the IdP. Alternatively, one RP's trust agreement could require that it use the home agency IdP, while another RP's trust agreement could allow for a secondary integration, such as a PKI federation gateway.

These decisions can also change over time. For example, an agency could deploy a new IdP service and transfer all existing accounts to it, or a trust agreement could point to different IdPs as new federation protocols are adopted and integrated.

2.2.2. Home Agency IdP

When a home agency officially endorses a specific PIV IdP for the PIV identity accounts that the agency issues, that IdP is known as the home agency IdP for that population of PIV identity accounts. The home agency IdP is often run by the home agency, but operations can be outsourced to a third party through a variety of technical means.

As discussed in Sec. 3.5, a home agency IdP has direct access to the home agency IdMS. This tight coupling allows the home agency IdP to be a highly trusted authority for the PIV identity account in question, including its current status and attributes. Not all use cases require a home agency IdP, but RPs can discover the home agency IdP for a given agency through the published home agency IdP record, as discussed in Sec. 3.5.

A particularly important application of the home agency IdP stems from non-PKI-based derived PIV credentials. These credentials can only be verified by the home agency, as discussed in [SP800-157]. However, if the home agency provides an IdP that can verify such credentials, the cardholder can authenticate to RPs outside of the home agency while using the non-PKI-based derived PIV credential as their primary authenticator.

2.2.3. Subscriber-Controlled wallets

The PIV IdP can be a subscriber-controlled wallet, as defined in [SP800-63C]. In this architecture, the IdP is issued a signed attribute bundle that represents the PIV identity account. This is done while the subscriber is authenticated using a PIV credential. The RP in turn trusts the assertions from the subscriber-controlled wallet thanks to the inclusion of the signed attribute bundle from a trusted source.

2.3. Relying Parties

In the context of a PIV federation, a subscriber logs into the RP using the federation protocol to use the RP's services and functionality. The nature of the services provided by the RP and the nature of the RP's deployment are outside the scope of this document. General requirements for the RP in a PIV federation are discussed in Sec. 5.3, and general requirements for RPs in all federation contexts are discussed in [SP800-63C].

In PIV federation, the RP does not directly verify the authentication of the PIV credential, nor does the RP manage the PIV identity account. The RP's only view into the contents and status of the PIV identity account comes through its interactions with the IdP. The RP can manage its own local reference to the PIV identity account along with information that is local to the RP. This record is known as the RP subscriber account and is defined by [SP800-63C] and discussed in Sec. 5.3.2.

At FAL3, the RP is also responsible for verifying the presentation of the bound authenticator, as discussed in [SP800-63C]. The bound authenticator could also be a PIV credential, but it is not necessary for it to be one (see Sec. 4.1.3 for more information about bound authenticators).

3. Trust Agreements

This section is normative.

The federation process defined in [SP800-63C] requires the establishment of a trust agreement between the RP and the IdP for the purpose of federated login, wherein the RP agrees to accept assertions from the IdP, and the IdP agrees to provide assertions and attributes to the RP.

In any PIV federation, the RP **SHALL** establish a single, specific IdP as the PIV IdP for a population of PIV identity accounts, as described in Sec. 2.2.1. The RP trusts this IdP to provide valid assertions for accounts within that population.

In many cases, the population is defined by the home agency of the PIV identity accounts, and the trust agreement defines a single PIV IdP for each home agency's accounts. It is possible — though uncommon — for an RP to have a distinct trust agreement established with an IdP for a single PIV identity account.

An RP in a PIV federation **SHALL** only accept assertions from PIV IdPs identified by its trust agreements. An RP **SHALL** reject assertions that do not comply with these trust agreements.

In addition to the requirements for trust agreements defined in [SP800-63C], trust agreements in PIV federation **SHALL** contain the following:

- A population of PIV identity accounts, including agency identifiers;
- A list of PIV IdPs or a process by which a PIV IdP is established by the home agency;
- The means for mapping a specific PIV identity account to a specific PIV IdP;
- The location of home agency IdP records for all agencies covered by the trust agreement, if applicable;
- The interoperable technical profile of the federation protocol in use; and
- The list of shared signals agreed to by all parties and the actions to be taken in response to receiving those signals.

When establishing a trust agreement, the RP **SHALL** disclose:

- The list of attributes requested and the purpose of use for each attribute,
- The population of PIV identity accounts associated with the IdP, and
- The possible range of AAL and FAL required to access the RP.

When establishing a trust agreement, the IdP **SHALL** disclose:

- The list of attributes that can be provided to an RP,
- The possible range of AAL and FAL supported by the IdP,
- Whether the IdP is the home agency IdP for the population PIV identity accounts (see Sec. 3.5), and
- The sources of attributes for the PIV identity accounts.

> Since all PIV accounts are IAL3, this attribute does not need to be otherwise disclosed.

Trust agreements between an RP and an IdP do not preclude different agreements being established with other parties. For example, an RP can have an agreement to accept IdP A as the PIV IdP for Agency X but have a separate agreement to accept IdP B as the PIV IdP for Agency Y. Both of these IdPs can likewise have trust agreements with many other RPs with potentially different parameters.

The trust agreement **SHALL** establish a deterministic process by which the RP can determine whether a given PIV identity account is included in the population of PIV identity accounts covered by a trust agreement and, therefore, whether the RP should accept an assertion from the IdP for that PIV identity account. The means for this determination are out of scope for these guidelines, but common mapping policies include mapping a single PIV IdP to PIV identity accounts that have the following attributes:

- All accounts from a single home agency, regardless of other attributes
- All accounts with a set of organizational affiliations
- All accounts with a particular job classification, such as full-time employees or contractors
- A specific set of accounts with known human-facing account identifiers, such as email addresses or phone numbers

The trust framework **MAY** stipulate that this mapping be made available through a queryable interface. For example, a federation authority can provide an interface that allows an RP to look up which IdP within the trust agreement to contact given a subscriber’s input to the RP.

The result of this process is a clear indication of which PIV identity accounts are served by which PIV IdP within the trust agreement. For example, an RP has established a trust agreement with IdP A as the PIV IdP for all subscribers from Agency X. If the RP then receives an assertion from IdP A for a subscriber from Agency Y, the RP would reject the assertion because the IdP is not trusted as the PIV IdP for Agency Y. Likewise, if the same

RP also has an established trust agreement with IdP B for a different agency, and the RP receives an assertion from IdP B for a subscriber from Agency X, the RP would reject that assertion because it has determined that IdP A is the PIV IdP for Agency X.

Any changes to the parameters of the trust agreement **SHALL** be documented and disclosed to affected parties. If the identified PIV IdP changes for one or more PIV identity accounts, the RP **SHALL** document any mappings made between federated identifiers for affected PIV identity accounts.

The trust agreement **SHALL** be established in either a bilateral fashion (see Sec. 3.1) directly between the parties or a multilateral fashion (see Sec. 3.2) through a federation authority, as described in the following sections.

3.1. Bilateral Agreements

An RP **MAY** enter a trust agreement directly with the PIV IdP in a bilateral fashion, as discussed in [SP800-63C].

When the PIV IdP is the home agency IdP for an agency, the home agency IdMS **SHALL** make its home agency IdP record available to the connected RP, as described in Sec. 3.5. The RP operator **SHALL** make the information in the home agency IdP record available to authenticated subscribers from that IdP upon request.

The IdP **SHOULD** make its discovery and registration available in a machine-readable format to facilitate configuration of the RP, as discussed in [SP800-63C].

3.2. Multilateral Agreements

Establishment of the trust agreement **MAY** be facilitated through the use of a trusted third party known as a federation authority, as discussed in [SP800-63C]. This creates a multilateral trust agreement between different PIV IdPs and RPs under the PIV federation authority. In such systems, the federation authority decides which PIV IdPs and RPs are allowed to participate based on the trust agreement provided by the authority. The federation authority **SHALL** declare which IdP is the PIV IdP for any given population of PIV identity accounts within the trust agreement. For all agencies covered by the federation authority's trust agreements, the federation authority **SHALL** indicate the agency's declared home agency IdP, if one exists.

The federation authority **SHALL** evaluate all PIV IdPs and RPs that sign on to a multilateral trust agreement with the federation authority to ensure that all parties adhere to the requirements of the trust agreement. The federation authority **SHALL** periodically reevaluate all members of the trust agreement. The schedule of evaluations **SHALL** be stipulated in the trust agreement.

The federation authority **SHALL** disclose to all connected RPs whether a particular IdP is the home agency IdP for a subscriber population. Federation authorities **SHALL** make all home agency IdP records (defined in Sec. 3.5) available to participants within the federation using a machine-readable format that is appropriate for the federation protocol standards in use. The federation authority **MAY** provide the home agency IdP records directly or through a pointer to a resource hosted by the home agency. As part of the trust agreement, the home agency **SHALL** document that its home agency IdP record is available through the federation authority in question.

The federation authority **SHALL** make lists of all member IdPs and RPs available to other members within the scope of the federation agreement. IdPs within a federation authority **SHOULD** enable dynamic registration of new RPs, as discussed in [SP800-63C], subject to the rules of the federation authority, the desired federation assurance level, and the capabilities of the federation protocol in use.

The federation authority **SHALL** document the full set of attributes that can be provided by each IdP and allowed to be requested by RPs within the federation. The federation authority **SHALL** collect the attributes requested by RPs joining the federation and **SHALL** document the RP's justification and use for these attributes.

3.3. Identity Proxies and Brokers

An identity proxy (also known as an identity broker) takes federated authentications from one domain and asserts them outbound to another domain, as discussed in [SP800-63C]. All requirements for proxies enumerated therein apply to identity proxies in a PIV federation.

Federation proxies can be used in both bilateral and multilateral trust agreements. While a federation authority facilitates the establishment of a trust agreement, it is not involved in the federation transaction. In contrast, an identity proxy facilitates the transaction itself by acting as a broker between the upstream IdP and downstream RP. In some cases, the same entity may operate both an identity proxy and a federation authority for all connected parties due to the proxy's nature as a common connection point between IdPs and RPs. Bilateral agreements are also possible through a proxy, with each IdP and RP making a pairwise trust agreement to the proxy itself.

For each federated transaction with an RP, the proxy **SHALL** determine the appropriate upstream PIV IdP that is appropriate for each PIV identity account it proxies to a downstream RP.

In addition to its other requirements as part of a trust agreement, an identity proxy in a PIV federation context **SHALL** disclose to other parties in the trust agreement that it is acting as a proxy. In its role as an IdP in a trust agreement, the proxy **SHALL** disclose to the RP the proxy's list of upstream PIV IdPs that the proxy uses as accounts for that RP within the trust agreement.

Assertions created by a proxy **SHALL** include the identifier of the upstream IdP. This is separate from the required issuer field, which identifies the proxy itself. Since the proxy is the issuer of federated assertions to its downstream RPs, these downstream RPs **SHALL** view the proxy as the PIV IdP for accounts asserted through the proxy.

3.4. Shared Signaling

In addition to sharing account information for the purposes of federated login, additional signals can be shared between the IdP and RP for the specific uses described in [SP800-63C].

The IdP **SHOULD** inform the RP of significant status changes in a PIV identity account that has been used at an RP, including:

- A suspected breach of the PIV identity account,
- The termination of the PIV identity account, or
- Changes to any part of the federated identifier.

When the RP receives such status changes, the RP **SHALL** update its RP subscriber account as specified by the trust agreement.

The IdP **MAY** additionally inform the RP of significant changes to the PIV identity account's information, including:

- A change in contact information attributes (email address, phone number),
- A change in primary authenticator status, or
- The addition or removal of secondary authenticator.

The RP **SHOULD** inform the IdP of significant status changes in the RP subscriber account, including:

- A suspected breach of the RP subscriber account or its data,
- Suspicious behavior of the RP subscriber account (e.g., repeated attempts to access unauthorized functions), or
- The addition or removal of RP-managed bound authenticators at FAL3.

When the IdP receives such a signal, the IdP **SHALL** update the account as specified by the trust agreement.

3.5. Home Agency IdPs

Only the home agency responsible for issuing PIV identity accounts **SHALL** declare the home agency IdP for those accounts. Operation of the home agency IdP **MAY** be outsourced to a third party, if the IdP meets the requirements in this section.

A home agency IdP **SHALL** have access to the PIV identity accounts that it represents through the home agency IdMS. Current access **SHALL** be available throughout the lifecycle of the PIV identity account while the home agency IdP is in operation. The access includes the following:

- All attributes available for federation,
- All PIV credentials bound to the account, and
- The current status of the PIV identity account (i.e., active/terminated).

The effect of these requirements is that the home agency IdP needs to be coupled to the home agency IdMS. This can be accomplished through a variety of technological means, such as direct attachment to the home agency IdMS or the use of a provisioning protocol to synchronize account state with the IdP system. In all cases, a home agency IdP is expected to have current, accurate, and authoritative information for all of the PIV identity accounts that it represents. Additionally, the IdP **SHALL** inform the home agency IdMS of any results of processing shared signals, as discussed in Sec. 3.4.

When declaring a home agency IdP, the home agency **SHALL** publish its home agency IdP record in a publicly available location that is securely associated with the home agency, such as on an HTTPS URL on the agency's domain or in a trusted directory service. The publication of the home agency IdP record **SHALL** include all of the following:

- A canonical issuer identifier for the IdP (generally a URI in federation protocols),
- A list of agency identifiers and organizational affiliations covered by the IdP,
- A list of federation protocols supported by the IdP along with any profiles of those protocols,
- The location of a machine-readable discovery document for each federation protocol supported by the IdP, and
- Technical contact information for the IdP.

The format for this record and the means by which it is published are out of scope for this specification and subject to technical profiles and federation trust agreements.

3.5.1. Home Agencies and Subscriber-Controlled Wallet

Subscriber-controlled wallets can be a trusted mechanism for PIV federation, even if they are not controlled by the home agency. The home agency can declare that subscriber-controlled wallets are sufficient to fulfill the role of a home agency IdP if the following are true:

- The home agency is able to validate the IdP software.
- The subscriber-controlled wallet can be deprovisioned by the home agency independent of IdP action.

To declare subscriber-controlled wallets as fulfilling a home agency IdP role, the home agency **SHALL** publish a record that indicates:

- A canonical identifier for the home agency onboarding subscriber-controlled wallets
- A list of public signing keys or the location of a machine-readable document that lists the public signing keys used to issue attribute bundles
- A list of agency identifiers and organizational affiliations covered by subscriber-controlled IdPs
- Technical contact information for the home agency

The keys listed in this record used for signing attribute bundles **SHALL NOT** be used for other purposes.

4. Federation Assurance Level (FAL)

This section is normative.

The federation assurance level, or FAL, is defined in [SP800-63C] as a set of requirements for the federation process. A higher FAL indicates a greater degree of trust that the RP can place in the results of the federation process—namely, that the subscriber present at the RP is the subscriber identified in the federation protocol.

As discussed in [SP800-63C], federation provides a means of conveying the proofing and authentication processes associated with the life cycle of the subscriber account. For PIV federation, the PIV identity account is proofed at IAL3, and all PIV credentials are either AAL2 or AAL3, depending on the type of credential. PIV federation **MAY** be conducted at any FAL, depending on the requirements of the use case.

4.1. Reaching Different FALs in PIV Federation

The FAL classification of a PIV federation transaction primarily depends on several aspects of the federation process, including the establishment of the trust agreement, as discussed in Sec. 3. [SP800-63C] defines general requirements for FALs, and this section defines requirements specific to PIV federation.

4.1.1. FAL1

FAL1 allows federation in a wide variety of situations, particularly when the results of a risk assessment show that the risk is low, and the value of making the federated connection outweighs the complexities of implementing higher FALs. The establishment of the trust agreement and the determination of the PIV IdP **MAY** be established at the behest of the subscriber. The PIV IdP **SHOULD** be the home agency IdP for the agency if the home agency IdP is known for the target agency by the RP. The RP **SHOULD** audit and review all accepted PIV IdPs.

As defined in [SP800-63C], at FAL1, the IdP **MAY** use front-channel presentation of the assertion. However, if the assertion contains private or sensitive information and is presented over the front-channel, an encrypted assertion **SHALL** be used.

4.1.2. FAL2

All of the requirements for FAL1 apply at FAL2 except when more specific or stringent requirements in this section override them.

As defined in [SP800-63C], FAL2 requires the assertion presentation to be protected against injection by an attacker at the RP. To accomplish this, PIV federation at FAL2 **SHALL** use back-channel presentation methods.

The establishment of the trust agreement and determination of the PIV IdP at FAL2 **SHALL** be performed prior to the start of the federation transaction. In this establishment, the RP **SHALL** ensure that the PIV IdP is the home agency IdP that represents the population of accounts in question. This process **MAY** be augmented by automated processes (e.g., key exchange) and facilitated by trusted parties (e.g., federation authority).

4.1.3. FAL3

All of the requirements for FAL1 and FAL2 apply at FAL3 except when more specific or stringent requirements in this section override them.

The PIV IdP at FAL3 **SHALL** establish identifiers and key material for RP such that the IdP can identify and trust the RP prior to the federation transaction.

As defined in [SP800-63C], FAL3 requires the establishment of a *bound authenticator*, which the subscriber presents directly to the RP alongside the federation assertion from the IdP. The bound authenticator does not need to be a PIV credential, though most PIV credentials can be used as bound authenticators at FAL3. When used as a bound authenticator, a PIV credential must be verified separately from the PIV identity account and the assertion with which it is associated. The nature of the binding depends on the type of authenticator, its use, and its phishing resistance qualities. The same authenticator **MAY** be used as both a derived PIV authenticator at the IdP and a bound authenticator at the RP in a single transaction provided that both the IdP and RP separately verify the authenticator.

PKI-based credentials, such as the PIV authentication certificate on the PIV Card, **MAY** be used as an IdP-managed bound authenticator, as shown in Fig. 2. When a certificate is used in this fashion, the assertion **SHALL** contain an identifier of the certificate (as discussed in Sec 6.2.3) as an attribute in the assertion to identify the specific certificate used as an authenticator. If the RP uses a just-in-time provisioning method for the RP subscriber account (as defined in [SP800-63C]), the RP **SHALL** compare the attributes of the certificate with other attributes from the federation transaction when first associating the bound authenticator with a federated identifier. For example, if the certificate includes one email address, and the federation transaction gives the RP a different email address, the RP needs to decide whether the transaction should be rejected or if this specific discrepancy is expected for its use case and security profile.

Non-PKI-based derived PIV credentials and authenticators other than PIV credentials **MAY** be used as RP-managed bound authenticators, as shown in Fig. 3, provided the authenticators meet the phishing resistance requirements in [SP800-63C]. With RP-managed bound authenticators, the IdP does not see the authenticator directly. The RP **SHALL** conduct an appropriate binding ceremony, as defined in [SP800-63C].

When a PIV credential is used as a bound authenticator at the RP, the RP **SHALL** verify the authenticator in the context of a valid assertion. In this way, the authenticator functions separately from its use as a PIV credential.

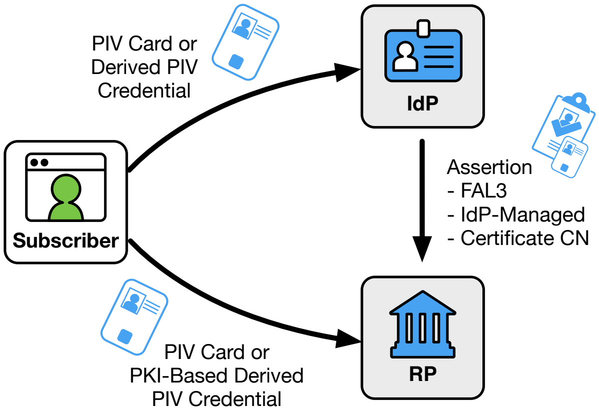

Fig. 2. IdP-managed bound authenticators

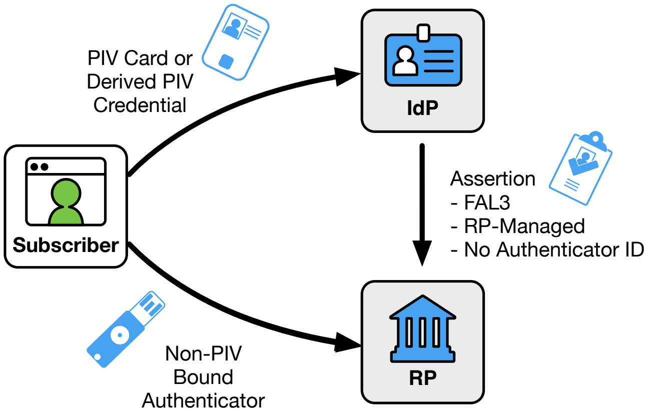

Fig. 3. RP-managed nound authenticators

In the case of a lost bound authenticator, the RP **SHALL** provide mechanisms for unbinding old authenticators and binding a new authenticator at FAL3.

4.2. Selecting FAL

Agencies **SHALL** select the FAL appropriate for a given RP using the digital identity risk management process specified in [SP800-63]. Notwithstanding the results of that process specifying a higher assurance level, agencies **SHOULD** use federation protocols, architectures, and processes that are compliant with FAL2 or higher to maximize the assurance provided by the management of the PIV identity accounts.

When not practical to deploy federation at FAL2 in low-impact use cases, agencies **MAY** elect to use FAL1 technologies and processes, in accordance with their digital identity risk management process. In such cases, the risk assessment **SHALL** consider the potential impact of risks associated with the FAL1 mechanisms that will be used. This could include assertion injection attacks associated with front-channel presentation mechanisms or acceptance of outdated attributes associated with use of PIV IdPs that are not the subjects’ home agency IdPs.

5. Requirements of IdPs and RPs

This section is normative.

This section details the requirements for IdPs and RPs in a PIV federation context.

5.1. General-Purpose IdP Requirements

PIV IdPs **SHALL** follow all requirements for general-purpose IdPs enumerated in [SP800-63C] in addition to the applicable requirements in this section.

All assertions generated by a PIV IdP **SHALL** follow the requirements enumerated in [SP800-63C]. In addition, all assertions for PIV federation need to follow the requirements in Sec. 6.2.

5.1.1. Authentication Requirements

The PIV IdP **SHALL** authenticate the subscriber using a valid and current PIV credential, which can be a PIV Card or derived PIV credential bound to the PIV identity account. Note that [FIPS201] specifies that derived PIV credentials must be bound to a PIV identity account by the issuing department or agency responsible for managing that PIV identity account. By implication, PIV IdPs operated by third parties must be in a position to verify the validity and currency of PIV credentials issued by the home agency. For PKI-based authenticators, this could be accomplished using PIV authentication certificates and the accompanying certificate status infrastructure. However, because non-PKI-based derived PIV credentials can only be verified by the home agency, PIV IdPs operated by third parties would need close integration with those issuing home agencies in order to be capable of verifying those authenticators.

The IdP **SHALL** issue an assertion within a valid session lifetime at the IdP, subject to the session management requirements of the IdP.

If the RP requests a maximum authentication age, the IdP **SHALL** reauthenticate the subscriber if the requested authentication age from the RP is not met by the subscriber’s current session at the IdP.

The IdP **SHALL** issue assertions only for PIV identity accounts that the IdP knows to be valid and current (e.g., the PIV identity account has not been terminated). To provide timely and accurate status information, home agency IdPs **SHOULD** derive this directly from the home agency’s authoritative records, such as its enterprise identity management system.

Note: for PIV IdPs using PKI-based PIV credentials as the only authenticators, the active status of the PIV identity account could be partially inferred from the validity of the certificate used for authentication. As long as revocation and expiration checks of the certificate are processed, a valid certificate is likely to indicate a valid PIV identity account. However, the certificate status does not necessarily reflect the status of the associated PIV identity account. A PIV certificate could be expired or revoked due to compromise for a cardholder whose PIV identity account remains in good standing. Additionally, the status of a certificate from a terminated PIV identity account may not be immediately reflected in the associated certificate revocation list, as Section 2.9.1 of [FIPS201] allows for 18 hours to complete the revocation process.

5.1.2. PIV Identity Account Identification

The IdP **SHALL** issue a unique federated identifier for each PIV identity account according to the requirements in Sec. 6.2.1, consisting of the logical combination of:

- A subject identifier for the PIV identity account that is locally unique for the account at the IdP, and
- A globally unique identifier for the IdP.

The federated identifier **SHOULD** be stable over time for a PIV identity account at an IdP. To protect privacy, the IdP **SHOULD** use an unguessable value for the subject identifier, such as the output from an approved random-number generator or a value derived from an approved derivation method for the subject. The federated identifier **SHALL NOT** contain any personally identifiable information or any personal identifiers, such as the cardholder UUID, in an unencrypted or reversible form.

5.1.3. Session Management

The IdP **SHALL** create a secure session with the subscriber after a successful authentication event with a PIV credential using session management, as described in [SP800-63B]. The IdP **SHALL** record the time of the last successful authentication event for a subscriber within the session associated with that subscriber. This time is used to calculate the authentication age of the session.

In managing the subscriber’s session at the IdP, the IdP **SHALL** follow all reauthentication guidelines as established in [SP800-63B] and [SP800-63C].

5.2. Subscriber-Controlled wallets

When using a subscriber-controlled wallet, the PIV IdP **SHALL** follow all requirements for subscriber-controlled wallets as defined in [SP800-63C]. The following additional requirements also apply:

- The subscriber **SHALL** authenticate using one or more PIV credentials during the IdP provisioning process
- The attribute bundle **SHALL** indicate that the account is a PIV account
- The attribute bundle **SHALL** indicate whether the subscriber-controlled wallet is considered a home agency IdP
- The attribute bundle **SHALL** indicate which FALs the subscriber-controlled wallet is authorized to act at

5.3. RP Requirements

PIV RPs **SHALL** follow all of the requirements for RPs enumerated in [SP800-63C].

5.3.1. Assertion Processing

The RP **SHALL** verify that all assertions contain all required elements as enumerated in Sec. 6.2. The RP **SHALL** reject any assertion that does not meet these requirements.

5.3.2. RP Subscriber Accounts

It is common practice for the RP to associate a federated login with a local account record. This record is defined as the RP subscriber account in [SP800-63C]. The RP subscriber account can contain things like access rights at the RP as well as a cache of identity attributes for the subscriber.

Each federated identifier, as described in Sec. 6.2.1, **SHALL** be associated with a single RP subscriber account. The RP subscriber account **SHALL NOT** rely on any other identifiers within the PIV data record (e.g., card UUID or email address) for uniqueness or tracking a PIV identity account over time.

The RP **MAY** associate multiple federated identifiers with a single RP subscriber account to perform account binding as discussed in [SP800-63C]. The RP **MAY** allow access to the RP subscriber account with a locally-verified authenticator, but when such an action is taken, access to the RP is not considered PIV federation.

To minimize the amount of information sent to the RP, RPs **SHOULD** use just-in-time provisioning for the RP subscriber account, as defined in [SP800-63C], when possible. To avoid data duplication and synchronization issues, the RP **SHOULD** minimize the amount of data stored in the RP subscriber account.

Note that it is possible for an RP to associate the same set of authorizations and attributes to two different RP subscriber accounts, depending on the needs of the RP. The means and details of doing so are outside the scope of this specification.

5.3.3. Session Management

The RP **SHALL** create a secure session with the subscriber upon successfully processing the assertion from the IdP. The RP **SHALL NOT** tie the session lifetime to the lifetime of the assertion. In common practice, the session lifetime at the RP is expected to outlive the validity window of the assertion.

The RP **SHALL** follow all session management requirements for RPs defined in [SP800-63C].

5.3.4. Changing the Federated Identifier

To facilitate recovery of an account when a federated PIV identity account can no longer be used, an RP **MAY** change the federated identifier bound to an RP subscriber account in limited circumstances to be recorded in the trust agreement:

- A change of PIV IdP for the home agency of a PIV identity account
- A change of configuration that alters the subject identifier or issuer identifier portion of the federated identifier for a PIV identity account

When the federated identifier is changed, the RP **SHALL** make the RP subscriber account inactive and **SHALL** require a succesful federated authentication using the new federated identifier before considering the RP subscriber account active again. The RP **SHALL NOT** allow the previously used federated identifier to be used to access the account.

The RP **SHALL** make a record of any such change, including the identifiers of all affected RP subscriber accounts at the time of the change. The RP **SHALL** provide notice to the subscriber when a federated identifier is bound or unbound to an RP subscriber account.

The RP **SHALL NOT** convert an RP subscriber account to be available using local authentication.

6. Protocol Requirements

This section is normative.

A federation protocol connects the IdP and RP together with a series of messages. These messages include assertions, which are passed between the IdP and RP to represent the federated authentication event, and the contents of identity APIs, which convey additional attribute information about the subscriber. This section enumerates requirements for these common components but is not intended to provide sufficient detail for any specific federation protocol.

6.1. Required Attributes

As stated in Sec. 3, the trust agreement establishes the set of attributes that the IdP provides to the RP and the purposes the RP has for those attributes. Some attributes are required to be available at the IdP. Some of the available attributes are mandatory to be provided to all RPs. Other attributes are available at the IdP but accessible only to RPs if stipulated in the trust agreement. Other attributes are optional for the IdP to have available, and likewise optional to be provided to RPs if stipulated in the trust agreement. The identity attributes found in the PIV identity account that are made available from a PIV IdP are not limited to those available from the PIV authentication certificate.

The following set of identity attributes **SHALL** be provided by a PIV IdP to every RP within any trust agreement for PIV federation:

- Subject Identifier: A unique identifier for the PIV identity account that is assigned by the IdP to the account for use by the RP. The subject identifier is part of the federated identifier (see Sec. 6.2.1 for additional requirements).
- Home Agency: A global identifier for the home agency associated with the PIV identity account (e.g., an agency’s domain name or a FASC-N agency code from [SP800-87]).
- Organizational Affiliation: The organization or list of organizations with which the PIV identity account is affiliated using global identifiers for the organization (e.g., an agency’s domain name or a FASC-N agency code from [SP800-87]). This can be the same as the home agency but may be different in practice. For example, an employee’s home agency may be the parent organization but their account is affiliated with the specific sub-organizations to which they are assigned.
- Last Updated: A timestamp that indicates when the available attributes in the PIV identity account were last updated at the IdP. (see Sec. 6.1.1.)

A PIV IdP **SHALL** have the following core identity attributes available as part of the account and **SHALL** make those attributes available to an RP if stipulated in the trust agreement:

- Full Name: The full name of the subscriber that is suitable for display or addressing the subscriber at the RP. Individual portions of the name (e.g., a given name or family name) **MAY** also be made available separately.

A PIV IdP **SHOULD** have the following core identity attributes available as part of the account and **SHOULD** make those attributes available to an RP if stipulated in the trust agreement:

- Email address: The current email address for the subscriber as known by or issued by the IdP
- Physical Address: The physical address of the subscriber, typically an office address
- Phone Number: The current telephone number for the subscriber as known by or issued by the IdP
- Certificate Identifier: The identifier of the PIV authentication certificate (see Sec 6.2.3)

Except as otherwise stated in Sec. 6.2, the IdP **SHOULD** disclose attributes through an identity API rather than through the assertion itself. For example, in OpenID Connect, while it is possible to include subscriber attributes such as `name` and `email` within the ID token (the assertion), it is preferable to make such attributes available from the UserInfo Endpoint (an identity API). When attributes are available for a given account through more than one method at an IdP, the attribute values **SHALL** match.

A PIV IdP **SHOULD** allow for selective disclosure of attributes to different RPs, as determined by the authorized party listed in the trust agreement.

6.1.1. Last Updated Time

The last updated attribute is provided as a hint to the RP about the current freshness of the attributes available from the IdP to allow the RP to decide when to refresh any attributes kept in the RP subscriber account.

The timestamp is calculated by the IdP, and its source varies depending on implementation. For example, for the home agency IdP, this would include any modifications made to the PIV identity account that affect the attributes that the IdP makes available. For other PIV IdPs, the last updated timestamp indicates when the IdP's copies of any attributes were last updated from their source. In all cases, the RP can track this timestamp as a value stored in the RP subscriber account. If the timestamp provided by the IdP is newer than that in the RP subscriber account, the RP can update its cached attributes from the IdP using any available mechanisms.

If multiple timestamps are available for different attributes, the latest timestamp **SHALL** be used.

6.2. Assertion Contents

As specified in [SP800-63C], the successful validation of a federated assertion is required to begin an authenticated session at the RP. The assertion contains a combination of attributes about the subscriber as well as attributes about the authentication event that the assertion represents.

At a minimum, the assertion in PIV federation **SHALL** contain the following attributes of the PIV identity account:

- Flag indicating that this assertion represents a PIV federation transaction
- Last updated timestamp for the PIV identity account
- Identifier for the home agency of the PIV identity account
- IAL for the PIV identity account (note that all PIV identity accounts are established at IAL3)
- Federated identifier for the PIV identity account at this IdP, as defined in Sec. 6.2.1

As an assertion is a short-lived message from the IdP to the RP, the assertion itself **SHOULD** only contain the minimum attributes required for its processing. To preserve privacy and minimize the information sent with each request, the assertion **SHOULD NOT** contain non-required or stable attributes from the PIV identity account (e.g., email address, display name). Additional attributes **SHOULD** be made available to the RP through a standard identity API.

At a minimum, the assertion in PIV federation **SHALL** contain the following attributes of the authentication event:

- AAL for the latest successful authentication event for the subscriber’s current session at the IdP
- Timestamp of the latest successful authentication event for the subscriber’s current session at the IdP
- Flag indicating whether the PIV Card or a derived PIV credential was used at the authentication event for the subscriber’s current session at the IdP
- Intended FAL for the current transaction

For FAL3 assertions in PIV federation, the assertion **SHALL** contain either:

- A reference to an IdP-managed bound authenticator to be verified by the RP (e.g., a certificate identifier, as discussed in Sec 6.2.3), or
- A flag indicating that an RP-managed bound authenticator is required at the RP.

The mapping of these required attributes to specific fields within a given federation protocol is out of scope for this specification.

6.2.1. Federated Identifier

The assertion created by a PIV IdP includes a *federated identifier* for the PIV identity account, as defined in [SP800-63C]. The federated identifier consists of the logical combination of both a *subject identifier* for the PIV identity account assigned by the IdP and a global *issuer identifier* for the IdP.

The subject identifier **SHALL** be unique to the PIV identity account at the IdP such that no identifier is the same for any two PIV identity accounts at an IdP.

The subject identifier **SHALL** be stable for a PIV identity account over time and **SHALL** survive common life cycle events, such as reissuance of a PIV Card or changes to attributes (e.g., email addresses, usernames).

The subject identifier **MAY** be generated by the IdP in a pairwise fashion for a specific RP, as discussed in [SP800-63C]. If such a pairwise identifier is used, it **SHALL** be used consistently with a given RP and **SHALL NOT** be used for multiple RPs except as allowed by [SP800-63C].

The subject identifier **SHALL NOT** include any personally identifiable or private information, such as a username, an certificate identifiers (see Sec 6.2.3), email addresses, the UUIDs of the PIV Card or cardholder, or an internal record number. These identifiers **MAY** be used as input to a one-way cryptographic function used to calculate a subject identifier. However, care should be taken to ensure that the resulting identifier is stable.

The issuer identifier **SHALL** be globally unique for the IdP. This identifier is usually the URL of the IdP, but it can also be a unique key identifier or other globally unique value that can be verified by the RP as part of the assertion.

The RP **SHALL** use this federated identifier to uniquely associate the PIV identity account with the RP subscriber account, as defined in [SP800-63C]. The RP **SHALL NOT** use other attributes alone for this purpose, including email addresses, certificate subject names, or PIV cardholder UUIDs.

6.2.2. Authorization and Access Rights

The assertion **MAY** contain indicators for the authorizations and access rights that the subscriber has at the RP, such as a set of roles within an organization. The RP **SHALL** trust these only as subject to the details of the trust agreements between the IdP and RP.

As the point of enforcement, the RP **MAY** override these authorizations by additionally restricting access as necessary.

6.2.3. Certificate Identifiers

The PIV authentication certificate is issued to PIV identity cardholders as part of the PIV Card and can uniquely identify a PIV identity account, as described in [FIPS201]. Within PIV federation, the PIV authentication certificate is not used for primary authentication to the RP, but it can still be referred to from the federation protocol in some important ways. For example, when used as an IdP-managed bound authenticator, the PIV authentication certificate is verified by both the PIV IdP and subsequently by the RP. For this to work, the assertion needs to communicate the identity of the certificate and its included keys in a reliable manner. The exact method of referring to the PIV authentication certificate is out of scope for this document and subject to profiling of the federation technology in use, but some common options include:

- The cryptographic hash of the public key used in the PIV authentication certificate,
- Certificate issuer (CA) and subject identifier
- CA and certificate serial number
- Subject key identifier
- The cryptographic hash of the full certificate
- The full certificate value

Each of these options has different tradeoffs and considerations, and an interoperable technical profile of this specification **SHOULD** define which of these are supported.

6.3. Discovery and Registration

The IdP **SHALL** publish its configuration information in a standard machine-readable format and location that are appropriate to the federation protocol in use. The information in the configuration document **SHALL** be sufficient to allow for the automated configuration of an RP contacting the IdP even when the RP is statically registered.

IdPs operating at FAL2 and below **SHOULD** allow RPs to register dynamically, as described in [SP800-63C]. Assertions issued to dynamically registered RPs **SHALL** contain pairwise subject identifiers.

6.4. Assertion Presentation

The IdP **SHALL** support back-channel assertion presentation, if possible within the federation protocol. All back-channel presentation methods **SHALL** require authentication of the RP.

At all FALs, RPs **SHOULD** use back-channel presentation to fetch the assertion directly from the IdP, where available.

If front-channel presentation is used and the assertion contains PII, the contents of the assertion **SHALL** be encrypted using a key specific to the RP, as required in [SP800-63C].

6.5. Attribute APIs

The IdP **SHALL** make identity attributes for the subscriber available through a standard identity API, if possible within the federation protocol in use. The identity API **SHALL** require protected access from the RP.

The IdP **SHALL** allow limited disclosure of attributes through this API, such that federation agreements that connect the IdP and RP (including runtime decisions by an authorized party) can dictate which attributes are disclosed to the RP for a given request.

The RP **SHALL** use the account update timestamp to manage its cache of attribute information in the RP subscriber account, particularly when using a just-in-time provisioning model. That is, if the account update timestamp in the assertion is later than the last cache update value, the RP knows that it should fetch updated information from the identity API. If the timestamp is not later than the cache time, the RP can determine that an additional call to the identity API would be redundant.

The IdP **MAY** provide a provisioning API to the RP, subject to a trust agreement. When a provisioning API is used, the trust agreement **SHALL** include a justification for the intended use of all attributes provided to the RP by the provisioning API.

6.6. Identity Proxies and Brokers

An identity proxy acting in a PIV federation context **SHALL** disclose the IdPs used as sources of attributes to the downstream RP. For example, if an assertion contains attributes for a PIV identity account from IdP A and IdP B, the proxy will list both IdPs as sources within the assertion. Note that the proxy, in its role as an IdP to downstream RPs, is still the issuer of the assertion and will identify itself as such.

See Sec. 3.3 for more information about the trust agreement requirements of identity proxies.

References

[FIPS201] National Institute of Standards and Technology (2022) *Personal Identity Verification (PIV) of Federal Employees and Contractors.* (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-3 [or as amended]. https://doi.org/10.6028/NIST.FIPS.201-3

[SP800-63] Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle C, Lefkovitz N, Regenscheid A (2024) *Digital Identity Guidelines.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4 2pd, 2024 [or as amended]. https://doi.org/10.6028/NIST.SP.800-63-4.2pd

[SP800-63B] Temoshok D, Fenton JL, Choong YY, Lefkovitz N, Regenscheid A, Richer JP (2024) *Digital Identity Guidelines: Authentication and Authenticator Management*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B-4 2pd, 2024 [or as amended]. https://doi.org/10.6028/NIST.SP.800-63b-4.2pd

[SP800-63C] Temoshok D, Richer JP, Choong YY, Fenton JL, Lefkovitz N, Regenscheid A (2024) *Digital Identity Guidelines: Federation and Assertions.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63C-4 2pd, 2024 [or as amended]. https://doi.org/10.6028/NIST.SP.800-63c-4.2pd

[SP800-87] Ferraiolo H (2018) *Codes for the Identification of Federal and Federally-Assisted Organizations*, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-87r2 [or as amended]. https://doi.org/10.6028/NIST.SP.800-87r2

[SP800-157] Ferraiolo H, Regenscheid AR, Fenton J (2024) *Guidelines for Derived Personal Identity Verification (PIV) Credentials.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-157 Revision 1 [or as amended]. https://doi.org/10.6028/NIST.SP.800-157r1-fpd

Appendix A. Examples

This appendix is informative.

This appendix contains several example scenarios of PIV federation in various environments and applications to show different kinds of trust establishment, account management, and authenticator usage. The details of the federation transactions within each scenario all follow the common patterns discussed in [SP800-63C] and adhere to the requirements in this document.

The scenarios in this section are for illustrative purposes and do not convey additional requirements beyond those imposed by this specification.

A.1. Direct Connection to the Home Agency IdP

Agency A, which issues and manages PIV identity accounts, sets up an OpenID Connect IdP in order to make its PIV identity accounts available online through a federation process. The agency publishes its home agency IdP record from its publicly available website with all of the information required by RPs to establish a connection.

The RP enters into a pairwise trust agreement with the IdP to accept assertions for Agency A. The RP declares the set of attributes that it needs from the IdP as part of this agreement. The RP uses a just-in-time provisioning system to establish an RP subscriber account when the subscriber logs in for the first time. The RP has other pairwise agreements with other IdPs to accept assertions for different agencies but will reject any assertions for accounts at Agency A that come from any other IdP.

The IdP generates a pairwise federated identifier for the PIV identity account for each RP that it is in contact with by hashing the identifier for the RP along with a randomly generated value stored with the PIV identity account at the IdP. This way, each new RP that signs on to the IdP gets a different federated identifier for a single account, but a consistent federated identifier is used for each RP with that account.

Per the terms of the trust agreement, the subscriber is prompted by the IdP the first time they log on to the RP. The IdP asks for the subscriber's consent at runtime to share attributes with the RP. The IdP prompts the subscriber to allow the IdP to remember this consent decision. This stored decision causes the IdP to act on the stored consent in a future request and not prompt the subscriber if the same RP requests the same attributes.

A.2. Multilateral Federation Network

Agencies A, B, and C each have a home agency IdP running OpenID Connect for their PIV identity accounts. All three agencies join a multilateral federation in which the federation authority independently verifies that each home agency IdP represents the agency in question. The federation authority publishes the home agency IdP records for all agencies that are part of the multilateral federation. This publication allows RPs within the federation to discover which IdP is to be used to access accounts for a given agency under the rules of the federation agreement.

RPs X and Y wish to allow logins from agencies A, B, and C, and the RPs declare their intent and a list of required attributes to the federation authority. The federation authority assesses both RP requests and adds them to the multilateral federation. This allows both RPs to register at each of the three separate IdPs as needed for each agency.

Both RPs interface directly with each of the three IdPs and not through a federation proxy. When a new IdP or RP is added to the multilateral federation agreement, the existing IdPs and RPs are notified of the new component and its parameters.

The IdPs and RPs establish a shared signaling channel under the auspices of the federation authority. This allows any IdP and any RP to report suspicious or malicious behavior that involves a specific account to the rest of the members under the federation authority.

A.3. Enterprise Application

The home agency IdP establishes a pairwise agreement with an RP to provide an enterprise-class service to the subjects of the agency’s PIV identity accounts. As part of this trust agreement, the home agency IdP allows access to a provisioning API for the RP. The provisioning API pushes a set of federated identifiers and associated attributes to the RP that allow the RP to pre-provision RP subscriber accounts for every PIV identity account at the IdP.

The existence of these RP subscriber accounts allows the RP to offer things like access rights, sharing, and messaging to all accounts on the system, whether or not the specific account has logged in to the RP yet.

Under the terms of the trust agreement, the RP is placed on an allowlist. Consequently, subscribers are not prompted for consent at runtime because the agency consented to use the service on behalf of all accounts at the time the RP was onboarded. This gives subscribers a seamless single sign-on experience, even though a federation protocol is being used across security domain boundaries. The RP can always request a re-authentication of the subscriber, resulting in a fresh assertion from the IdP.

The RP subscriber accounts are synchronized using the provisioning API. When a new PIV identity account is created, modified, or deleted at the IdP, the IdP updates the status of the RP subscriber account using the provisioning API. This allows the RP to always have an up-to-date status for each PIV identity account. For example, when the subscriber account is terminated at the IdP, the provisioning API signals to the RP that the RP subscriber account is to be terminated immediately. The RP removes all locally cached attributes for the account in question, except for the identifiers and references in audit and access logs.

A.4. PKI-Based Federation Gateway

A service provider that does not issue any PIV identity account of its own sets up a SAML IdP that accepts PKI-based PIV credentials as its only authentication method. These accounts are provisioned at the IdP using the attributes in the certificates when the subscriber first presents the certificate. The IdP collects no additional attributes from the subscriber in the process.

The IdP generates federated identifiers for the accounts by computing a hash of the authentication certificate and encoding that hash in Base64. This process fulfills the requirements of this document for federated identifiers, but it is specific to this IdP and need not be known or understood by any RP connecting through the IdP. If the subscriber changes any attributes in the certificate (e.g., their name), then a new federated identifier will be created as a result. As a result, this IdP does not necessarily provide a stable subject identifier across authenticator updates.

The RP enters into a pairwise trust agreement with the IdP to accept assertions for any agency with PIV credentials. The RP does not have any other IdPs that it speaks to directly, and so the only way to log in to the RP is through this gateway. Since the IdP accepts a broad range of PKI-based credentials, this allows the RP access to any account based on those credentials.

This setup does not allow the PIV identity accounts to use non-PKI-based derived PIV credentials since the IdP portion of the gateway is not the home agency IdP for any of the accounts in question. The RP is also not able to receive any attributes other than those available directly to the IdP through subscriber certificates. To ensure account continuity, an RP would need to have an out-of-band process to bind their new federated identifier to the existing RP subscriber account if the certificate and attributes change over time.

The IdP is not acting as a federation proxy because the inbound credential is not a federated assertion but rather a PKI-based credential that the gateway processes directly as a verifier.

A.5. PIV Federation Proxy as a Federation Authority

A federation proxy is set up within a multilateral federation. The proxy is run by the federation authority. All IdPs under the multilateral agreement register the proxy as an RP. The RPs within the federation authority connect to the proxy as their only IdP. All federation transactions within the multilateral federation flow through the proxy.

The federation authority discloses the nature of the proxy to all parties, so the IdPs know that this particular RP is a proxy, and the RPs know that their IdP is a proxy. Furthermore, the proxy lists all of the upstream IdPs and their associated populations of PIV identity accounts to all RPs connecting through the proxy.

The proxy discloses to the RPs which upstream IdPs participated in the authentication of the PIV identity account to the proxy, allowing the downstream RPs to validate that the source of the federation transaction through the proxy is appropriate for the PIV identity account in question.

The proxy is not regarded as a home agency IdP for any RP in the system, even if the IdPs connecting to the proxy are themselves home agency IdPs.

A.6. FAL3 With a PIV Card and PKI-Based Derived PIV Credentials

The PIV Card and certain PKI-based derived PIV credentials can be used as IdP-managed bound authenticators for use at FAL3. The home agency IdP authenticates the PIV identity account using an authenticator bound to the account and then creates an assertion that is flagged as FAL3. The assertion also contains the certificate common name (CN) and thumbprint of the certificate to be used as a bound authenticator.

When the RP receives the assertion, it processes it as usual and sees the FAL3 flag and the certificate attributes. The RP matches the CN against attributes in the RP Subscriber Account to ensure that the certificate being identified is appropriate for the PIV identity account being represented. The RP then prompts the subscriber to authenticate using a certificate and compares that certificate against the provided CN and thumbprint, ensuring that they match. When the certificate has been validated, the RP creates a secure session at FAL3. From this point forward in the session, the RP no longer requires presentation of the certificate in order to access the RP’s services.

A.7. FAL3 With an RP-Bound Authenticator

The home agency IdP authenticates the PIV identity account using an authenticator bound to the account, and then creates an assertion that is flagged as FAL3 and using an RP-bound authenticator.

When the RP receives the assertion, it processes it as usual and sees the FAL3 flag. The RP looks up the bound authenticator associated with the RP Subscriber Account and prompts the subscriber for this authenticator. When the authenticator has been verified, the RP creates a secure session at FAL3.

A.8. Issuance to a Digital Wallet

The home agency provides a service to issue PIV-account-backed credentials to digital wallets. This home agency has decided to accept any wallet as capable of issuing credentials at FAL1. During issuance, the subscriber logs in to the home agency’s issuing endpoint using their PIV Card. The subscriber activates their wallet and presents it to the home agency, which issues a signed attribute bundle to the wallet representing the PIV identity account.

During the federated transaction, the subscriber presents their wallet to the RP to log in. The RP requests an assertion from the wallet, which is acting as the IdP. The subscriber activates the wallet, and the wallet issues an assertion and delivers it to the RP. The RP looks up the home agency’s attribute bundle signing keys and validates the signed attribute bundle based on those keys. The RP then validates the assertion based on the key included in the signed attribute bundle.

Appendix B. Glossary of Terms

This section is informative.

home agency
The agency responsible for the issuance and management of a PIV identity account. Also known as the issuing agency, with regard to the PIV identity account.

home agency identity management system (IdMS)
The identity management system that stores and manages the PIV identity account, its associated attributes, and PIV credential bindings.

home agency identity provider (IdP)
The officially sanctioned identity provider of the home agency for a PIV identity account.

identity provider (IdP)
The party that verifies the credentials of a subscriber account and issues assertions to an RP based on that account for federation.

organizational affiliation
The list of organizations affiliated with a PIV identity account. This is often the same as the home agency, but can be different in practice.

PIV credential
A PIV Card or derived PIV credential.

PIV federation
A federation process that presents a PIV identity account from a PIV IdP. The subscriber is authenticated at the IdP using PIV credentials.

PIV identity provider (IdP)
An identity provider that accepts PIV credentials as authenticators for PIV identity accounts as part of PIV federation. The IdP trusted by the RP to create assertions for a PIV identity account.

relying party (RP)
The party that accepts an assertion from an IdP to allow the federated login of a PIV identity account.

Appendix C. Abbreviations

This section is informative.

AAL
Authentication Assurance Level

API
Application Programming Interface

CSP
Credential Service Provider

FAL
Federation Assurance Level

FASC-N
Federal Agency Smart Credential Number

IAL
Identity Assurance Level

IdP
Identity Provider

IdMS
Identity Management System

PKI
Public Key Infrastructure

PIV
Personal Identity Verification

RP
Relying Party