

Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date November 14, 2024

Original Release Date January 10, 2023

The attached draft document is followed by:

Status Final Public Draft (fpd)

Series/Number NIST SP 800-217 fpd

Title Guidelines for Personal Identity Verification (PIV) Federation

Publication Date November 2024

DOI <https://doi.org/10.6028/NIST.SP.800-217.fpd>

CSRC URL <https://csrc.nist.gov/pubs/sp/800/217/fpd>

Additional Information



1

NIST Special Publication NIST SP 800-217 ipd

2

3

Guidelines for Personal Identity Verification (PIV) Federation

4

5

Initial Public Draft

6

Hildegard Ferraiolo

7

Andrew Regenscheid

8

Justin P. Richer

9

This publication is available free of charge from:

10

<https://doi.org/10.6028/NIST.SP.800-217.ipd>

11

12 NIST Special Publication
13 NIST SP 800-217 ipd

14 Guidelines for Personal Identity
15 Verification (PIV) Federation

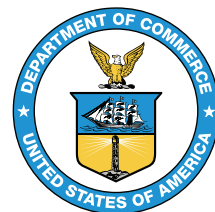
16 Initial Public Draft

17 Hildegard Ferraiolo
18 Andrew Regenscheid
19 *Computer Security Division*
20 *Information Technology Laboratory*

21 Justin P. Richer
22 *Bespoke Engineering*

23 This publication is available free of charge from:
24 <https://doi.org/10.6028/NIST.SP.800-217.ipd>

25 January 2023



27 U.S. Department of Commerce
28 *Gina M. Raimondo, Secretary*

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

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

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

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

46 **Authority**

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

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

62 **NIST Technical Series Policies**

63 [Copyright, Fair Use, and Licensing Statements](#)
64 [NIST Technical Series Publication Identifier Syntax](#)

65 **Publication History**

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

68 **How to Cite this NIST Technical Series Publication**

69 Ferraiolo H, Regenscheid A, Richer JP (2023) Guidelines for Personal Identity
70 Verification (PIV) Federation. (National Institute of Standards and Technology,
71 Gaithersburg, MD), NIST Special Publication (SP) 800-217 ipd. [https://doi.org/10.6028/
72 NIST.SP.800-217.ipd](https://doi.org/10.6028/NIST.SP.800-217.ipd)

73 **Author ORCID iDs**

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

77 **Public Comment Period**

78 January 10, 2023 - ~~March 24~~ April 21, 2023

79 **Submit Comments**

80 mailto:piv_comments@nist.gov

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

83 **Reports on Computer Systems Technology**

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

95 **Abstract**

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

105 **Keywords**

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

109 **Note to Reviewers**

110 The family of PIV credentials includes a variety of form factors and authenticator
111 types – as envisioned in OMB Memoranda M-19-22 and M-22-09 and subsequently
112 outlined in FIPS 201-3. The cross-domain and interagency use of these credentials is
113 provided by federation protocols outlined in this public draft SP 800-217 *Guidelines for*
114 *PIV Federation*. The companion document, SP 800-157r1 *Guidelines for Derived PIV*
115 *Credentials*, details the authenticators themselves. Both documents are closely aligned
116 with draft release SP 800-63-4 *Digital Identity Guidelines*. NIST hopes that the draft
117 document enable a close alignment with new and emerging digital identity and federation

118 technologies employed in the federal government, while maintaining a strong security
119 posture.

120 NIST is specifically interested in comments on and recommendations for the following
121 topics:

122 **Home Agency Attributes:**

- 123 • Are additional attributes needed in the guidelines to achieve interagency or cross-
124 domain interoperability?
- 125 • Are additional attributes required for RP provisioning and access?

126 **PIV Federation:**

- 127 • Are additional process steps or mechanism needed for the connection and
128 communication between home-IdP-to PIV identity account?
- 129 • Do the required parameters for establishing trust agreements fit the use cases for
130 PIV RPs?
- 131 • Are the required identity attributes sufficient for PIV use cases?
- 132 • Are the federated subject identifier requirements sufficient for PIV use cases?
- 133 • Is it clear how to apply the binding ceremony for RP-managed bound authenticators
134 at FAL3 to PIV and non-PIV authenticators?

135 Reviewers are encouraged to comment on all or part of both SP 800-157r1 and SP 800-
136 217. NIST requests that all comments be submitted by 11:59pm Eastern Time on March
137 24, 2023. Please submit your comments to piv_comments@nist.gov. NIST will review
138 all comments and make them available at the [NIST Computer Security Resource Center](#)
139 [website](#). Commenters are encouraged to use the comment template provided with the
140 [document announcement](#).

141 **Call for Patent Claims**

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

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

- 151 a) assurance in the form of a general disclaimer to the effect that such party does not
152 hold and does not currently intend holding any essential patent claim(s); or
- 153 b) assurance that a license to such essential patent claim(s) will be made available
154 to applicants desiring to utilize the license for the purpose of complying with the
155 guidance or requirements in this ITL draft publication either:
 - 156 i. under reasonable terms and conditions that are demonstrably free of any unfair
157 discrimination; or
 - 158 ii. without compensation and under reasonable terms and conditions that are
159 demonstrably free of any unfair discrimination.

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

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

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

169	Table of Contents	
170	1. Introduction	1
171	1.1. Background	1
172	1.2. Purpose and Scope	2
173	1.3. Federation Use Cases	2
174	1.3.1. Federation Considerations	3
175	1.4. Audience	4
176	1.5. Notations	4
177	1.6. Document Structure	4
178	2. Architecture	6
179	2.1. PIV Identity Account	7
180	2.2. Identity Providers	7
181	2.2.1. Home IdP	8
182	2.2.2. PIV IdP	9
183	2.3. PIV Credentials	9
184	2.4. Relying Parties	9
185	3. Trust Agreements	11
186	3.1. Bilateral Agreements	12
187	3.2. Multilateral Agreements	12
188	3.3. Identity Proxies and Brokers	13
189	3.4. Shared Signaling	14
190	3.5. Home IdPs	15
191	4. Federation Assurance Level (FAL)	16
192	4.1. Reaching Different FALs in PIV Federation	16
193	4.1.1. FAL1	16
194	4.1.2. FAL2	16
195	4.1.3. FAL3	17
196	4.2. Selecting FAL	19
197	5. Requirements of IdPs and RPs	20
198	5.1. IdP Requirements	20

199	5.1.1. Authentication Requirements	20
200	5.1.2. PIV Identity Account Identification	21
201	5.1.3. Session Management	21
202	5.2. RP Requirements	21
203	5.2.1. Assertion Processing	21
204	5.2.2. RP Subscriber Accounts	22
205	5.2.3. Session Management	22
206	5.2.4. Changing the Federated Identifier	22
207	6. Protocol Requirements	24
208	6.1. Required Attributes	24
209	6.2. Assertion Contents	25
210	6.2.1. Federated Identifier	26
211	6.2.2. Authorization and Access Rights	27
212	6.3. Discovery and Registration	27
213	6.4. Assertion Presentation	27
214	6.5. Attribute APIs	27
215	6.6. Identity Proxies and Brokers	28
216	References	29
217	Appendix A. Examples	30
218	A.1. Direct Connection to the Home IdP	30
219	A.2. Multilateral Federation Network	30
220	A.3. Enterprise Application	31
221	A.4. PKI-Based Federation Gateway	32
222	A.5. PIV Federation Proxy as a Federation Authority	32
223	A.6. FAL3 With a PIV Card	33
224	A.7. FAL3 With an RP-Bound Authenticator	33
225	Appendix B. Glossary of Terms	34
226	Appendix C. Abbreviations	35

227	List of Figures	
228	1. PIV Federation	6
229	2. IdP-Managed Bound Authenticators	18
230	3. RP-Managed Bound Authenticators	18

231 **1. Introduction**

232 *This section is informative.*

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

243 **1.1. Background**

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

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

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

260 Note that this document is not intended to be sufficient for a full technical interoperability
261 profile. In addition to this document and its prerequisites ([FIPS201] and [SP800-63C]), a
262 PIV federation deployment will need a technical profile that is suitable for the federation
263 protocol being used. For example, while this document requires that the federated
264 identifier be included in the assertion, a technical profile would specify the field name
265 within the assertion to house both the subject identifier and issuer identifier, as well as any
266 data formatting needed for the value.

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 lifecycle 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.

1.3. Federation Use Cases

In a *direct authentication*, the claimant presents their authenticator to a verifier, which is tightly coupled with the RP and often the Credential Service Provider (CSP). The verifier conducts an authentication process. 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.

Since the IdP needs to perform the role of verifier, usually the IdP is a service directly provided by the CSP. 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 an IdP to be run by a party other than the CSP. For example, the CSP could outsource the IdP functionality and synchronize the state of its PIV identity accounts using a provisioning protocol or similar system. Alternatively, the use of PKI-based PIV credentials allows an IdP to be run by a party other than the CSP. In this scenario, the validity of the PIV identity account is inferred from the validity of the credential presented to the third-party IdP.

303 **1.3.1. Federation Considerations**

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

311 Federation allows an RP to access PIV identity accounts that originate from different
312 agencies on different networks. This connection allows an agency to leverage the identity
313 infrastructure of another agency without needing to replicate the PIV identity account
314 management process.

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

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

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

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

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

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

348 **1.4. Audience**

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

351 **1.5. Notations**

352 This Standard uses the following typographical conventions in text:

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

368 **1.6. Document Structure**

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

- 371 • Section 2 describes a general architecture for PIV federation. This section is
372 *informative*.
- 373 • Section 3 describes the trust agreements in a PIV federation. This section is
374 *normative*.

- 375 • Section 4 describes the Federation Assurance Levels as applied to PIV federation.
376 This section is *normative*.
- 377 • Section 5 describes the requirements for IdPs and RPs in a PIV federation. This
378 section is *normative*.
- 379 • Section 6 describes the requirements for protocol elements in a PIV federation,
380 including assertion contents. This section is *normative*.
- 381 • References contains a list of publications referred to from this document. This
382 section is *informative*.
- 383 • Appendix A contains a glossary of selected terms used in this document. This
384 appendix is *informative*.
- 385 • Appendix B contains a selected list of abbreviations used in this document. This
386 appendix is *informative*.

387 **2. Architecture**

388 *This section is informative.*

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

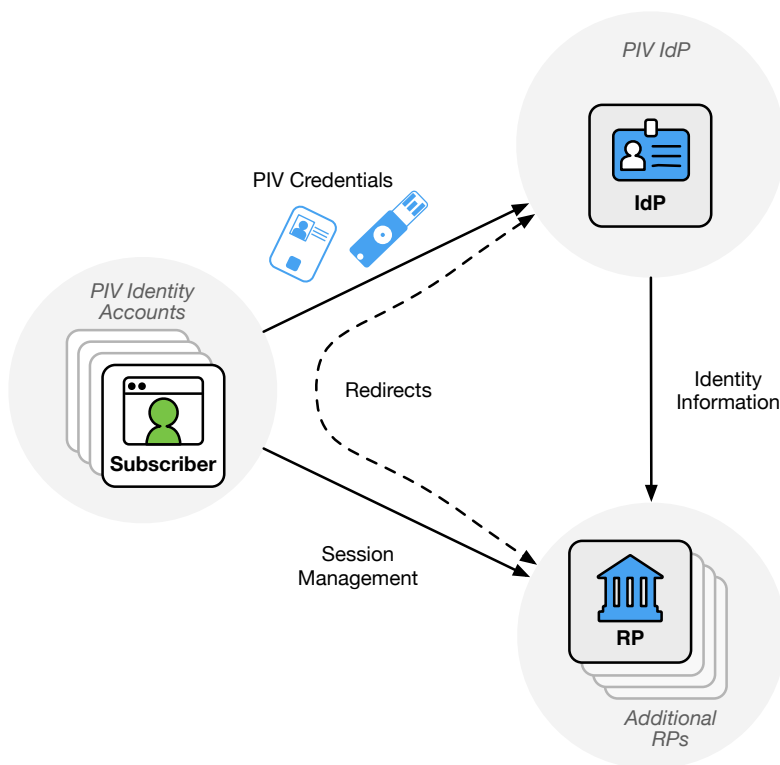


Figure 1. PIV Federation

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

- 396 • The account being asserted is a valid and active PIV identity account (See [Sec. 2.1](#)).
- 397 • The RP has established the IdP as the PIV IdP for the account through a valid and
398 current trust agreement (See [Sec. 2.2.2](#)).
- 399 • The subscriber authenticates to the IdP using a PIV credential (See [Sec. 2.3](#)).

400 If any of these items are not true, such as the use of a non-PIV identity account at a PIV-
401 enabled IdP or the authentication of a PIV identity account through an IdP that is not

402 the PIV IdP for the account, then the transaction does not meet the requirements of PIV
403 federation, and therefore the definitions and requirements in this document do not apply.

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

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

414 **2.1. PIV Identity Account**

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

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

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

429 **2.2. Identity Providers**

430 As described in [SP800-63C], the IdP is a service of the Credential Service Provider
431 (CSP) that issues and maintains the PIV identity account. In a federation transaction, the
432 IdP acts as the verifier for the authenticator held by the subscriber. In the case of PIV
433 federation, this means that the IdP verifies the PIV credential bound to the PIV identity
434 account, as discussed in Sec. 2.3.

435 The IdP sends a cryptographically verifiable message called an *assertion* to the RP that
436 identifies the PIV identity account being authenticated. The assertion contains attributes

437 associated with that PIV identity account and details about the authentication event, as
438 discussed in [Sec. 6.2](#). The IdP can also make PIV identity account attributes available
439 through a protected identity API alongside the assertion, as discussed in [Sec. 6.5](#).

440 The *home IdP* (see [Sec. 2.2.1](#)) is the IdP operated by or on behalf of the issuer of a
441 PIV identity account, which is typically expected to be the agency employing a federal
442 employee or contractor. As a consequence, the home IdP has a direct view of the
443 management of the PIV identity account and PIV credentials associated with the account,
444 including PKI-based and non-PKI-based authenticators. Because there may be multiple
445 IdPs capable of issuing assertions for a PIV cardholder, some of whom may not be
446 directly linked to the PIV identity account, each issuer will need to identify the home
447 IdP for the cardholders they serve, as discussed in [Sec 3.5](#).

448 A *PIV IdP* is the IdP trusted by an RP to issue assertions for a given PIV identity account.
449 From the perspective of the RP, all PIV federation transactions involve a PIV IdP. A PIV
450 IdP is trusted by the RP to issue accurate and timely assertions regarding a PIV identity
451 account. When the PIV IdP is not the home IdP, the account status can be ascertained by
452 other means, such as querying the PIV identity account issuer or inferring account status
453 from the status of the PKI-based PIV credential used to authenticate to the PIV IdP.

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

463 **2.2.1. Home IdP**

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

468 As discussed in [Sec. 3.5](#), a home IdP has direct access to the PIV identity account. This
469 tight coupling allows the home IdP be a highly trusted authority for the PIV identity
470 account in question.

471 Not all use cases require a home IdP, but RPs can discover the home IdP for a given
472 agency through the published home IdP record, as discussed in [Sec. 3.5](#).

473 Note that the use of a home IdP is the only means of making non-PKI-based derived
474 PIV credentials available across security domain boundaries due to the nature of the
475 authenticators, as discussed in [SP800-157].

476 **2.2.2. PIV IdP**

477 The PIV IdP is the PIV IdP identified in a trust agreement to provide federated assertions
478 for a population of PIV identity accounts for an RP. Establishment of the PIV IdP is
479 discussed in greater detail in [Sec. 3](#).

480 In most cases, the RP's determination of the PIV IdP depends on the agency that issues
481 the PIV identity account. Therefore, an RP will only accept assertions of PIV identity
482 accounts of a particular agency from a specific IdP. However, it is possible for the RP to
483 be more specific and determine the PIV IdP on a per-account basis, subject to the trust
484 agreements in place.

485 It is possible for an RP's definition of the PIV IdP for a given PIV identity account to
486 change over time as the federation relationship changes for a variety of reasons, including
487 reorganization of the PIV identity account's issuing agency or redeployment of the IdP.

488 **2.3. PIV Credentials**

489 PIV identity accounts are protected using one or more PIV credentials that are bound to
490 the account. PIV credentials can take the form of different kinds of authenticators, each
491 kind suitable for different purposes and use cases.

492 The primary credential for a PIV identity account is the PIV Card, which is issued to the
493 subscriber, as defined in [\[FIPS201\]](#).

494 A PIV identity account can also have multiple derived PIV credentials associated with it,
495 as described in [\[SP800-157\]](#).

496 **2.4. Relying Parties**

497 In the context of a PIV federation, a subscriber logs into the RP using the federation
498 protocol to use the RP's services and functionality. The nature of the services provided
499 by the RP and the nature of the RP's deployment are outside the scope of this document.
500 General requirements for the RP in a PIV federation are discussed in [Sec. 5.2](#), and general
501 requirements for RPs in all federation contexts are discussed in [\[SP800-63C\]](#).

502 In PIV federation, the RP does not directly verify the authentication of the PIV credential,
503 nor does the RP manage the PIV identity account. The RP's only view into the contents
504 and status of the PIV identity account comes through its interactions with the IdP. The
505 RP can manage its own local reference to the PIV identity account, known as the RP
506 subscriber account, as discussed in [Sec. 5.2.2](#).

507 At FAL3, the RP is responsible for verifying the presentation of the bound authenticator,
508 as discussed in [\[SP800-63C\]](#). Note that the bound authenticator could also be a PIV
509 credential, but it is not necessary for it to be one (see [Sec. 4.1.3](#) for more information
510 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 specific IdP as the PIV IdP for a population of PIV identity accounts, as described in Sec. 2.2.2. The RP **SHALL** trust this IdP to provide valid assertions for accounts within that population. In many cases, the population is defined by the issuing agency of the PIV identity accounts, and the trust agreement defines a single PIV IdP for each issuing 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** accept assertions only from PIV IdPs identified by its trust agreements. An RP **SHALL** accept assertions only within the bounds of its established trust agreements. An RP **SHALL** reject assertions that do not comply with these trust agreements.

Trust agreements in PIV federation **SHALL** consist of the following:

- A population of PIV identity accounts under consideration, including agency identifiers;
- A list of PIV IdPs and the PIV identity accounts they represent;
- A list of RPs capable of receiving assertions from the PIV IdPs;
- The authorized party, as defined in [SP800-63C]; and
- The interoperable technical profile of the federation protocol in use.

When establishing a trust agreement, the RP **SHALL** disclose to the PIV IdP or federation authority:

- The list of attributes requested and the purpose of use for each attribute;
- The possible range of IAL, AAL, and FAL required to access the RP; and
- The means for mapping any relevant PIV identity account to a specific PIV IdP.

When establishing a trust agreement, the IdP **SHALL** disclose to the RP or federation authority:

- The list of attributes provided;
- The possible range of IAL, AAL, and FAL supported by the IdP;

- 544 • Whether the IdP is the home IdP for the population PIV identity accounts (see
545 [Sec. 3.5](#)); and
- 546 • The sources of attributes for the PIV identity accounts.

547 For example, an RP has established a trust agreement with IdP A as the PIV IdP for
548 all subscribers from Agency X. If the RP then receives an assertion from IdP A for a
549 subscriber from Agency Y, the RP would reject the assertion because the IdP is not
550 trusted as the PIV IdP for Agency Y. Likewise, if the same RP also has an established
551 trust agreement with IdP B, and the RP receives an assertion from IdP B for a subscriber
552 from Agency X, the RP would reject that assertion because it has established IdP A as the
553 PIV IdP for this agency.

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

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

563 The trust agreement **SHALL** be established in either a bilateral fashion (See [Sec. 3.1](#))
564 directly between the parties or a multilateral fashion (See [Sec. 3.2](#)) through a federation
565 authority, as described in the sections below.

566 **3.1. Bilateral Agreements**

567 An RP **MAY** establish the PIV IdP directly with the IdP in a bilateral fashion, as
568 discussed in [\[SP800-63C\]](#).

569 When the PIV IdP is the home IdP for an agency, the PIV IdP operator **SHALL** make
570 available its home IdP record to the connected RP, as described in [Sec. 3.5](#). The RP
571 operator **SHALL** make the home IdP record available to authenticated subscribers from
572 that IdP, upon request.

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

575 **3.2. Multilateral Agreements**

576 An RP **MAY** establish the PIV IdP through the use of a trusted third party known as a
577 federation authority, as discussed in [\[SP800-63C\]](#). This creates a multilateral agreement
578 between different PIV IdPs and RPs under the PIV federation authority. In such systems,
579 the federation authority decides which PIV IdPs and RPs are allowed to participate

580 based on the trust agreement provided by the authority. The federation authority **SHALL**
581 declare which IdP is the PIV IdP for any given population of PIV identity accounts within
582 the trust agreement. The federation authority **SHALL** establish and declare whether each
583 PIV IdP is the home IdP for any given PIV identity account within the trust agreement.

584 The federation authority **SHALL** vet all PIV IdPs and RPs within the federation to ensure
585 that all parties are acting within the terms of the agreements.

586 The federation authority **SHALL** disclose to all connected RPs whether a particular IdP
587 is the home IdP for an agency in question. Federation authorities **SHALL** make all home
588 IdP records (defined in [Sec. 3.5](#)) available to participants within the federation using a
589 machine-readable format appropriate for the federation protocol standards in use.

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

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

599 **3.3. Identity Proxies and Brokers**

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

604 In many cases, it is natural for a proxy to act as a federation authority for all connected
605 parties due to the proxy's nature as a common connection point between IdPs and RPs.
606 However, bilateral agreements are still possible and allowable through a proxy, with each
607 IdP and RP making a pairwise agreement to the proxy itself.

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

611 In addition to its other requirements as part of a trust agreement, an identity proxy
612 in a PIV federation context acting as an IdP **SHALL** disclose to the RP or federation
613 authority:

- 614 • The proxy's nature as a proxy and
- 615 • The list of PIV IdPs that the proxy connects to for accounts that the RP is able to
616 access.

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

621 **3.4. Shared Signaling**

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

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

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

630 When the RP receives such status changes, the RP **SHOULD** update its RP subscriber
631 account, as appropriate for the nature of the signal.

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

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

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

- 639 • A suspected breach of the RP subscriber account or its data,
- 640 • Suspicious behavior of the RP subscriber account (such as repeated attempts to
641 access unauthorized functions), or
- 642 • The addition or removal of RP-managed bound authenticators at FAL3.

643 When the IdP receives such status changes, the IdP **SHOULD** terminate, disable, or
644 update the PIV identity account or the RP's access to the account as appropriate to the
645 nature of the signal.

646 **3.5. Home IdPs**

647 Only the agency responsible for issuing PIV identity accounts **SHALL** declare the home
648 IdP for those accounts. Operation of the home IdP **MAY** be outsourced to a third party.

649 A home IdP **SHALL** have access to relevant information for the PIV identity accounts
650 that it asserts, including the following:

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

654 The effect of these requirements is that the home IdP needs to be coupled to the
655 management of the PIV identity accounts that it represents. This can be accomplished
656 with a variety of technological means, such as attachment to the issuing agency's
657 enterprise identity and access management system or the use of a provisioning protocol to
658 synchronize account state with the IdP system.

659 The issuing agency responsible for declaring its home IdP **SHALL** publish its home IdP
660 information in a publicly available location to allow for discovery and configuration by
661 RPs. The home IdP publication record **SHALL** include all of the following:

- 662 • A canonical issuer identifier for the IdP (this is generally a URI in federation
663 protocols),
- 664 • A list of agency identifiers covered by the IdP,
- 665 • A list of federation protocols supported by the IdP along with any profiles of those
666 protocols,
- 667 • The location of a machine-readable discovery document for each federation
668 protocol supported by the IdP, and
- 669 • Technical contact information for the IdP.

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

672 **4. Federation Assurance Level (FAL)**

673 *This section is normative.*

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

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

683 **4.1. Reaching Different FALs in PIV Federation**

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

688 **4.1.1. FAL1**

689 FAL1 allows federation in a wide variety of situations, particularly where the results of
690 a risk assessment show that the value of making the federated connection outweighs the
691 complexities of implementing higher FALs. The establishment of the trust agreement and
692 the determination of the PIV IdP **MAY** happen dynamically. The PIV IdP **SHOULD** be
693 the home IdP for the agency if known by the RP. The RP **SHOULD** audit and review all
694 accepted PIV IdPs.

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

698 **4.1.2. FAL2**

699 All of the requirements for FAL1 apply at FAL2 except where overridden by more
700 specific or stringent requirements in this section.

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

704 The establishment of the trust agreement and determination of the PIV IdP at FAL2
705 **SHALL** be done through a trusted process whereby the RP ensures that the PIV IdP
706 is the official home IdP that represents the population of accounts in question. This

707 process **MAY** be augmented by automated processes, including dynamic discovery
708 and registration of the identifiers and key material for the IdP and RP in the federation
709 protocol.

710 **4.1.3. FAL3**

711 All of the requirements for FAL1 and FAL2 apply at FAL3 except where overridden by
712 more specific or stringent requirements in this section.

713 Trust establishment of the PIV IdP at FAL3 **SHALL** be done through a trusted process
714 whereby the RP ensures that the PIV IdP is the official home IdP that represents the
715 agencies and accounts in question. The establishment of identifiers and key material for
716 the IdP and RP in the federation protocol **SHALL** occur through a static process between
717 the IdP and RP.

718 As defined in [SP800-63C], FAL3 requires the establishment of a *bound authenticator*,
719 which the subscriber presents directly to the RP alongside the federation assertion from
720 the IdP. Though most PIV credentials can be used as bound authenticators at FAL3,
721 the nature of the binding depends on the type of authenticator, its use, and its phishing
722 resistance qualities.

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

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

739 In their use as bound authenticators at FAL3, authenticators from PIV credentials do not
740 function as PIV credentials at the RP. However, the same authenticator **MAY** be used as
741 both a derived PIV authenticator at the IdP and a bound authenticator at the RP in a single
742 transaction provided that both the IdP and RP separately verify the authenticator.

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

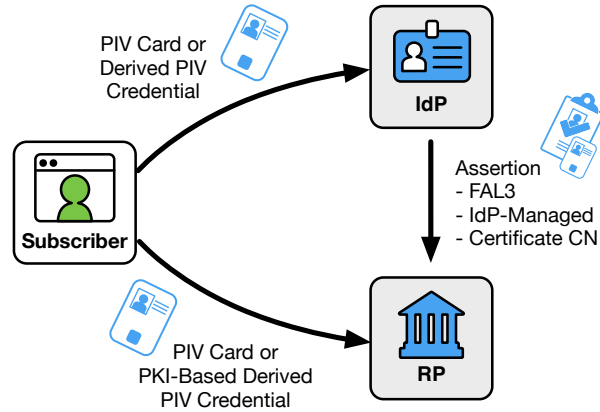


Figure 2. IdP-Managed Bound Authenticators

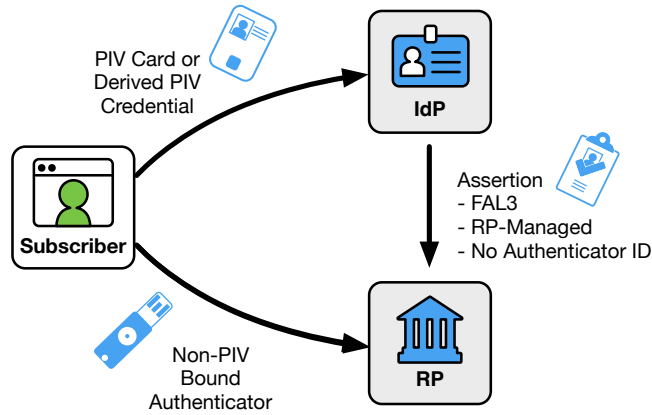


Figure 3. RP-Managed Bound Authenticators

745 **4.2. Selecting FAL**

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

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

PIV IdPs **SHALL** follow all requirements for 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 only 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 still 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 on be verified by the issuing home agency, PIV IdPs operated by third parties would need close integration with those issuing home agencies to capable of verifying those authenticators.

The IdP **SHALL** issue an assertion within a valid session lifetime at the IdP. The IdP **SHOULD** require a recent successful authentication with a PIV credential.

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 and associated PIV card have not been terminated). To provide timely and accurate status information, home IdPs **SHOULD** derive this directly from the issuing agency's authoritative records, such as its enterprise identity management system. For other PIV IdPs using PKI-based PIV credentials as the only authenticators, the status of the PIV identity account could be inferred from the validity of the certificate used for authentication, including revocation and expiration checks. Note that 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. Similarly, a

794 terminated PIV identity account will not be immediately reflected in associated certificate
795 revocation lists.

796 **5.1.2. PIV Identity Account Identification**

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

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

802 To protect privacy, the IdP **SHOULD** use a cryptographically random value or a
803 cryptographically derived value for the subject identifier portion of the federated
804 identifier. The federated identifier **SHALL NOT** contain any personally identifiable
805 information or any personal identifiers, such as the cardholder UUID, in an unencrypted
806 or reversible form. The federated identifier **SHOULD** be stable over time for a PIV
807 identity account at an IdP.

808 **5.1.3. Session Management**

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

814 In managing the subscriber's session at the IdP, the IdP **SHALL** follow all
815 reauthentication guidelines as established in [\[SP800-63B\]](#) and [\[SP800-63C\]](#).

816 When using PKI-based authenticators such as PIV authentication certificates, an IdP
817 **SHOULD** require presentation of the certificate for only a specific path that represents the
818 explicit authentication event. This configuration mirrors the verification process for other
819 forms of authenticators and enables the use of a secure session.

820 **5.2. RP Requirements**

821 PIV RPs **SHALL** follow all of the requirements for RPs enumerated in [\[SP800-63C\]](#).

822 **5.2.1. Assertion Processing**

823 The RP **SHALL** verify that all assertions received contain the requirements enumerated in
824 [Sec. 6.2](#). The RP **SHALL** reject any assertion that does not meet these requirements.

825 **5.2.2. RP Subscriber Accounts**

826 It is common practice for the RP to associate that login with a local account record, which
827 is defined as the RP subscriber account in [SP800-63C].

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

832 The presentation of two distinct federated identifiers to the same RP **SHALL** be treated as
833 two distinct PIV identity accounts from the perspective of that RP.

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

838 The RP **SHALL NOT** allow access to the RP account outside of the context of a verified
839 assertion from a trusted IdP. This includes local authentication with an authenticator
840 known to the RP.

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

844 **5.2.3. Session Management**

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

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

851 **5.2.4. Changing the Federated Identifier**

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

- 855 • A change of PIV IdP for the issuing agency of a PIV identity account
- 856 • A change of configuration that alters the subject identifier or issuer identifier
857 portion of the federated identifier for a PIV identity account

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

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

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

869 **6. Protocol Requirements**

870 *This section is normative.*

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

877 **6.1. Required Attributes**

878 A PIV IdP **SHALL** make the following mandatory attributes available to all RPs for each
879 PIV identity account, as required by the trust agreement:

- 880 • **Subject Identifier:** A unique identifier for the PIV identity account that is assigned
881 by the IdP to the account for use by the RP; the subject identifier is part of the
882 federated identifier, see [Sec. 6.2.1](#) for additional requirements.
- 883 • **Issuing Agency:** A global identifier for the issuing agency associated with the PIV
884 identity account (e.g., an agency's domain name or a FASCN agency code from
885 [\[SP800-87\]](#)).
- 886 • **Organizational Affiliation:** The organization or list of organizations that the PIV
887 identity account is affiliated with.
- 888 • **Last Updated:** A timestamp that indicates when the available attributes in the PIV
889 identity account were last updated at the IdP.

890 A PIV IdP **SHALL** make the following core identity attributes available to RPs, subject to
891 the trust agreement:

- 892 • **Email address:** The current email address for the subscriber as known by or issued
893 by the IdP.
- 894 • **Full Name:** The full name of the subscriber that is suitable for display or addressing
895 the subscriber at the RP; the individual portions of the name, such as a given name
896 and family name, **MAY** also be made available separately.

897 A PIV IdP **SHOULD** make the following optional identity attributes available to RPs,
898 subject to the trust agreement:

- 899 • **Physical Address:** The physical address of the subscriber, most typically an office
900 address
- 901 • **Phone Number:** The current telephone number for the subscriber as known by or
902 issued by the IdP

- 903 • Certificate Subject Distinguished Name Field: The Subject Distinguished Name
904 field of the subscriber's current PIV authentication certificate

905 Any given RP does not necessarily have access to all attributes made available by
906 an IdP. The subject identifier (and therefore the federated identifier), issuing agency,
907 organizational affiliations, and last updated timestamp **SHALL** be disclosed as part of all
908 trust agreements in PIV federations. All other subscriber account attributes are subject to
909 the trust agreement in place between the IdP and RP, including disclosures of use between
910 the parties.

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

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

919 **6.2. Assertion Contents**

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

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

- 926 • Flag indicating that this assertion represents a PIV federation transaction
- 927 • Last updated timestamp for the PIV identity account
- 928 • Identifier for the issuing agency of the PIV identity account
- 929 • IAL for the PIV identity account (which is IAL3)
- 930 • Federated identifier for the PIV identity account at this IdP, as defined in [Sec. 6.2.1](#)

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

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

- 939 • AAL for the latest successful authentication event for the subscriber's current
940 session at the IdP
- 941 • Timestamp of the latest successful authentication event for the subscriber's current
942 session at the IdP
- 943 • Flag indicating whether the PIV Card or a derived PIV credential was used at the
944 authentication event for the subscriber's current session at the IdP
- 945 • Intended FAL for the current transaction

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

- 947 • A reference to an IdP-managed bound authenticator to be verified by the RP (such
948 as the Subject Distinguished Name of the PIV Card authentication certificate), or
- 949 • A flag indicating that an RP-managed bound authenticator is required at the RP.

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

952 **6.2.1. Federated Identifier**

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

957 The subject identifier **SHALL** be unique to the PIV identity account at the IdP such that
958 no identifier is the same for any two PIV identity accounts at an IdP. The subject identifier
959 **MAY** be generated by the IdP in a pairwise fashion for a specific RP, as discussed in
960 [SP800-63C]. If such a pairwise identifier is used, it **SHALL** be used consistently with a
961 given RP and **SHALL NOT** be used for multiple RPs except as allowed by [SP800-63C].

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

965 The federated identifier **SHALL NOT** include any personally identifiable or private
966 information, such as username, identifier, the distinguished name of the PIV
967 authentication certificate, email addresses, or UUIDs for the PIV Card or cardholder.

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

972 **6.2.2. Authorization and Access Rights**

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

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

978 **6.3. Discovery and Registration**

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

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

986 **6.4. Assertion Presentation**

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

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

992 If front-channel presentation is used, the contents of the assertion **SHALL** be encrypted to
993 a key specific to the RP, as described in [SP800-63C].

994 **6.5. Attribute APIs**

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

998 The IdP **SHALL** allow limited disclosure of attributes through this API, such that
999 federation agreements that connect the IdP and RP (including runtime decisions by an
1000 authorized party) can dictate which attributes are disclosed to the RP for a given request.

1001 The RP **SHALL** use the account update timestamp to manage its cache of attribute
1002 information in the RP subscriber account, particularly when using a just-in-time
1003 provisioning model. That is, if the account update timestamp in the assertion is later than
1004 the last cache update value, the RP knows that it should fetch updated information from
1005 the identity API. If the timestamp is not later than the cache time, the RP can determine
1006 that an additional call to the identity API would be redundant.

1007 The IdP **MAY** provide a provisioning API to the RP, subject to a trust agreement. When
1008 a provisioning API is used, the trust agreement **SHALL** include a justification for the
1009 intended use of all attributes provided to the RP by the provisioning API.

1010 **6.6. Identity Proxies and Brokers**

1011 An identity proxy acting in a PIV federation context **SHALL** disclose the IdPs used
1012 as sources of attributes to the downstream RP. For example, if an assertion contains
1013 attributes for a PIV identity account from IdP A and IdP B, the proxy will list both IdPs as
1014 sources within the assertion. Note that the proxy, in its role as an IdP to downstream RPs,
1015 is still the issuer of the assertion and will identify itself as such.

1016 See [Sec. 3.3](#) for more information about the trust agreement requirements of identity
1017 proxies.

1018 **References**

- 1019 **[FIPS201]** National Institute of Standards and Technology (2022) *Personal Identity*
1020 *Verification (PIV) of Federal Employees and Contractors*. (U.S. Department of
1021 Commerce, Washington, DC), Federal Information Processing Standards Publication
1022 (FIPS) 201-3 [or as amended]. <https://doi.org/10.6028/NIST.FIPS.201-3>
- 1023 **[SP800-63]** Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle
1024 C, Lefkovitz N, Regenscheid A (2022) *Digital Identity Guidelines*. (National Institute of
1025 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4
1026 ipd, 2022 [or as amended]. <https://doi.org/10.6028/NIST.SP.800-63-4.ipd>
- 1027 **[SP800-63B]** Temoshok D, Fenton JL, Choong YY, Lefkovitz N, Regenscheid A, Richer
1028 JP (2022) *Digital Identity Guidelines: Authentication and Lifecycle Management*.
1029 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
1030 Publication (SP) 800-63B-4 ipd, 2022 [or as amended]. <https://doi.org/10.6028/NIST.SP.800-63b-4.ipd>
- 1032 **[SP800-63C]** Temoshok D, Richer JP, Choong YY, Fenton JL, Lefkovitz N, Regenscheid
1033 A (2022) *Digital Identity Guidelines: Federation and Assertions*. (National Institute of
1034 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63C-4
1035 ipd, 2022 [or as amended]. <https://doi.org/10.6028/NIST.SP.800-63c-4.ipd>
- 1036 **[SP800-87]** Ferraiolo H (2018) *Codes for the Identification of Federal and Federally-*
1037 *Assisted Organizations*, (National Institute of Standards and Technology, Gaithersburg,
1038 MD), NIST Special Publication (SP) 800-87r2 [or as amended]. [https://doi.org/10.6028/](https://doi.org/10.6028/NIST.SP.800-87r2)
1039 [NIST.SP.800-87r2](https://doi.org/10.6028/NIST.SP.800-87r2)
- 1040 **[SP800-157]** Ferraiolo H, Regenscheid AR, Fenton J (2023) *Guidelines for Derived*
1041 *Personal Identity Verification (PIV) Credentials*. (National Institute of Standards and
1042 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-157 Revision 1 [or as
1043 amended]. <https://doi.org/10.6028/NIST.SP.800-157r1-ipd>

1044 **Appendix A. Examples**

1045 *This appendix is informative.*

1046 This appendix contains several example scenarios of PIV federation in various
1047 environments and applications to show different kinds of trust establishment, account
1048 management, and authenticator usage. The details of the federation transactions within
1049 each scenario all follow the common patterns discussed in [SP800-63C] and adhere to the
1050 requirements in this document.

1051 The scenarios in this section are for illustrative purposes and do not convey additional
1052 requirements beyond those imposed by this specification.

1053 **A.1. Direct Connection to the Home IdP**

1054 Agency A, which issues and manages PIV identity accounts, sets up an OpenID Connect
1055 IdP in order to make its PIV identity accounts available online through a federation
1056 process. The agency publishes its home IdP record from its publicly available website
1057 with all required information for RPs to consume.

1058 The RP enters into a pairwise trust agreement with the IdP to accept assertions for
1059 Agency A. The RP declares the set of attributes that it needs from the IdP as part of this
1060 agreement. The RP uses a just-in-time provisioning system to establish an RP subscriber
1061 account only once the subscriber logs in for the first time. The RP has other pairwise
1062 agreements with other IdPs to accept assertions for different agencies but will reject any
1063 assertions for accounts at Agency A that come from any other IdP.

1064 The IdP generates a pairwise federated identifier for the PIV identity account for each
1065 RP that it is in contact with by hashing the identifier for the RP along with a randomly
1066 generated value stored with the PIV identity account at the IdP. This way, each new RP
1067 that signs on to the IdP gets a different federated identifier for a single account, but a
1068 consistent federated identifier is used for each RP with that account.

1069 Per the terms of the trust agreement, the subscriber is prompted by the IdP the first
1070 time they log on to the RP. The IdP asks for the subscriber's consent at runtime to share
1071 attributes with the RP. The IdP also prompts the subscriber to allow the IdP to remember
1072 this consent decision. This stored decision causes the IdP to act on the stored consent in a
1073 future request and not prompt the subscriber if the same RP requests the same attributes.

1074 **A.2. Multilateral Federation Network**

1075 Agencies A, B, and C each have a home IdP running OpenID Connect for their PIV
1076 identity accounts. All three agencies join a multilateral federation in which the federation
1077 authority independently verifies that each home IdP represents the agency in question.
1078 The federation authority publishes the home IdP records for all agencies that are part of
1079 the multilateral federation. This publication allows RPs within the federation to discover

1080 which IdP is to be used to access accounts for a given agency under the rules of the
1081 federation agreement.

1082 RPs X and Y wish to allow logins from agencies A, B, and C, and the RPs declare their
1083 intent and a list of required attributes to the federation authority. The federation authority
1084 assesses both RP requests and adds them to the multilateral federation. This allows both
1085 RPs to register at each of the three separate IdPs as needed for each agency.

1086 Both RPs interface directly with each of the three IdPs and not through a federation proxy.
1087 When a new IdP or RP is added to the multilateral federation agreement, the existing IdPs
1088 and RPs are notified of the new component and its parameters.

1089 The IdPs and RPs establish a shared signaling channel under the auspices of the
1090 federation authority. This allows any IdP and any RP to report suspicious or malicious
1091 behavior that involves a specific account to the rest of the members under the federation
1092 authority.

1093 **A.3. Enterprise Application**

1094 The home IdP establishes a pairwise agreement with an RP to provide an enterprise-
1095 class service to the subjects of the agency's PIV identity accounts. As part of this trust
1096 agreement, the home IdP allows access to a provisioning API for the RP. The provisioning
1097 API pushes a set of federated identifiers and associated attributes to the RP that allow the
1098 RP to pre-provision RP subscriber accounts for every PIV identity account at the IdP.

1099 The existence of these RP subscriber accounts allows the RP to offer things like access
1100 rights, sharing, and messaging to all accounts on the system, whether or not the specific
1101 account has logged in to the RP yet.

1102 Under the terms of the trust agreement, the RP is placed on an allowlist. Consequently,
1103 subscribers are not prompted for consent at runtime because the agency consented to
1104 use the service on behalf of all accounts at the time the RP was onboarded. This gives
1105 subscribers a seamless single sign-on experience, even though a federation protocol is
1106 being used across security domain boundaries.

1107 The RP subscriber accounts are synchronized using the provisioning API. When a new
1108 PIV identity account is created, modified, or deleted at the IdP, the IdP updates the status
1109 of the RP subscriber account using the provisioning API. This allows the RP to always
1110 have an up-to-date status for each PIV identity account. For example, when the RP
1111 subscriber account is terminated at the IdP, the provisioning API signals to the RP that
1112 the RP subscriber account is to be terminated immediately. The RP removes all locally
1113 cached attributes for the account in question, except for the identifiers and references in
1114 audit and access logs.

1115 **A.4. PKI-Based Federation Gateway**

1116 A service provider that does not issue any PIV identity account of its own sets up a
1117 SAML IdP that accepts PKI-based PIV credentials as its only authentication method.
1118 These accounts are provisioned at the IdP using the attributes in the certificates when the
1119 subscriber first presents the certificate. The IdP collects no additional attributes from the
1120 subscriber in the process.

1121 The IdP generates federated identifiers for the accounts by computing a hash of the
1122 authentication certificate and encoding that hash in Base64. This process fulfills the
1123 requirements of this document for federated identifiers, but it is specific to this IdP and
1124 need not be known or understood by any RP connecting through the IdP. Note that if
1125 the subscriber changes any attributes in the certificate, such as their name, then a new
1126 federated identifier will be created as a result. As a result, this IdP does not necessarily
1127 provide a stable subject identifier across authenticator updates.

1128 The RP enters into a pairwise trust agreement with the IdP to accept assertions for any
1129 agency with PIV credentials. The RP does not have any other IdPs that it speaks to
1130 directly, and so the only way to log in to the RP is through this gateway. Since the IdP
1131 accepts a broad range of PKI-based credentials, this allows the RP access to any account
1132 based on those credentials.

1133 This setup does not allow the PIV identity accounts to use non-PKI-based derived
1134 PIV credentials since the IdP portion of the gateway is not the home IdP for any of the
1135 accounts in question. The RP is also not able to receive any attributes other than those
1136 available directly to the IdP through subscriber certificates. To ensure account continuity,
1137 an RP would need to have an out-of-band process to bind their new federated identifier to
1138 the existing RP subscriber account if the certificate and attributes change over time.

1139 The IdP is not acting as a federation proxy because the inbound credential is not a
1140 federated assertion but rather a PKI-based credential that the gateway processes directly
1141 as a verifier.

1142 **A.5. PIV Federation Proxy as a Federation Authority**

1143 A federation proxy is set up within a multilateral federation. The proxy is run by the
1144 federation authority. All IdPs under the multilateral agreement register the proxy as an
1145 RP. The RPs within the federation authority connect to the proxy as their only IdP. All
1146 federation transactions within the multilateral federation flow through the proxy.

1147 The federation authority discloses the nature of the proxy to all parties, so the IdPs know
1148 that this particular RP is a proxy, and the RPs know that their IdP is a proxy. Furthermore,
1149 the proxy lists all of the upstream IdPs and their associated populations of PIV identity
1150 accounts to all RPs connecting through the proxy.

1151 The proxy discloses to the RPs which upstream IdPs participated in the authentication of
1152 the PIV identity account to the proxy, allowing the downstream RPs to validate that the

1153 source of the federation transaction through the proxy is appropriate for the PIV identity
1154 account in question.

1155 The proxy is not regarded as a home IdP for any RP in the system, even if the IdPs
1156 connecting in to the proxy are themselves home IdPs.

1157 **A.6. FAL3 With a PIV Card**

1158 The PIV Card and certain PKI-based derived PIV credentials can be used as IdP-managed
1159 bound authenticators for use at FAL3. The home IdP authenticates the PIV identity
1160 account using an authenticator bound to the account and then creates an assertion that
1161 is flagged as FAL3. The assertion also contains the certificate common name (CN) and
1162 thumbprint of the certificate to be used as a bound authenticator.

1163 When the RP receives the assertion, it processes it as usual and sees the FAL3 flag and
1164 the certificate attributes. The RP matches the CN against attributes in the RP Subscriber
1165 Account to ensure that the certificate being identified is appropriate for the PIV identity
1166 account being represented. The RP then prompts the subscriber to authenticate using a
1167 certificate and compares that certificate against the provided CN and thumbprint, ensuring
1168 that they match. When the certificate has been validated, the RP creates a secure session
1169 at FAL3. From this point forward in the session, the RP no longer requires presentation of
1170 the certificate in order to access the RP's services.

1171 **A.7. FAL3 With an RP-Bound Authenticator**

1172 The home IdP authenticates the PIV identity account using an authenticator bound to the
1173 account, and then creates an assertion that is flagged as FAL3 and using an RP-bound
1174 authenticator.

1175 When the RP receives the assertion, it processes it as usual and sees the FAL3 flag. The
1176 RP looks up the bound authenticator associated with the RP Subscriber Account and
1177 prompts the subscriber for this authenticator. When the authenticator has been verified,
1178 the RP creates a secure session at FAL3.

1179 **Appendix B. Glossary of Terms**

1180 *This section is informative.*

1181 **Home Agency**

1182 The agency responsible for the issuance and management of a PIV identity account.

1183 **Home IdP**

1184 The officially sanctioned IdP of the home agency for a PIV identity account.

1185 **Identity Provider (IdP)**

1186 The party that verifies the credentials of a subscriber account and issues assertions to an
1187 RP based on that account for federation.

1188 **PIV Credential**

1189 A PIV Card or derived PIV credential.

1190 **PIV Federation**

1191 A federation process that presents a PIV identity account from a PIV IdP. The subscriber
1192 is authenticated at the IdP using PIV credentials.

1193 **PIV IdP**

1194 An IdP that accepts PIV credentials as authenticators for PIV identity accounts as part of
1195 PIV federation. The IdP trusted by the RP to create assertions for a PIV identity account.

1196 **Relying Party (RP)**

1197 The party that accepts an assertion from an IdP to allow the federated login of a PIV
1198 identity account.

1199 **Appendix C. Abbreviations**

1200 *This section is informative.*

1201 **AAL**

1202 Authentication Assurance Level

1203 **API**

1204 Application Programming Interface

1205 **CSP**

1206 Credential Service Provider

1207 **FAL**

1208 Federation Assurance Level

1209 **FASC-N**

1210 Federal Agency Smart Credential Number

1211 **IAL**

1212 Identity Assurance Level

1213 **IdP**

1214 Identity Provider

1215 **PKI**

1216 Public Key Infrastructure

1217 **PIV**

1218 Personal Identity Verification

1219 **RP**

1220 Relying Party