



1

NIST Special Publication 800 NIST SP 800-217 fpd

2

3

Guidelines for Personal Identity Verification (PIV) Federation

4

5

Final 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.fpd>

11

12 **NIST Special Publication 800**
13 **NIST SP 800-217 fpd**

14 **Guidelines for Personal Identity**
15 **Verification (PIV) Federation**

16 **Final 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.fpd>

25 November 2024



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
32 document in order to describe an experimental procedure or concept adequately. Such
33 identification is not intended to imply recommendation or endorsement by the National
34 Institute of Standards and Technology, nor is it intended to imply that the entities,
35 materials, or 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
53 federal officials exercising policy authority over such systems. This guideline is consistent
54 with 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
57 under statutory authority. Nor should these guidelines be interpreted as altering or
58 superseding the existing authorities of the Secretary of Commerce, Director of the
59 OMB, or any other federal official. This publication may be used by nongovernmental
60 organizations on a voluntary basis and is not subject to copyright in the United States.
61 Attribution would, 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 final
67 publication]

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

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

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 November 14, 2024 - January 10, 2025

79 **Submit Comments**

80 mailto:piv_comments@nist.gov

81 **Additional Information**

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

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

85 **Abstract**

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

95 **Keywords**

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

99 **Reports on Computer Systems Technology**

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

111 **Call for Patent Claims**

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

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

- 121 a) assurance in the form of a general disclaimer to the effect that such party does not
122 hold and does not currently intend holding any essential patent claim(s); or
- 123 b) assurance that a license to such essential patent claim(s) will be made available
124 to applicants desiring to utilize the license for the purpose of complying with the
125 guidance or requirements in this ITL draft publication either:
 - 126 i. under reasonable terms and conditions that are demonstrably free of any
127 unfair discrimination; or
 - 128 ii. without compensation and under reasonable terms and conditions that are
129 demonstrably free of any unfair discrimination.

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

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

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

140 **Table of Contents**

| | | |
|-----|-----------------------------------------------------------------------|-----------|
| 141 | 1. Introduction | 1 |
| 142 | 1.1. Background | 1 |
| 143 | 1.2. Purpose and Scope | 1 |
| 144 | 1.2.1. Creating Technical Interoperability Profiles of This Guideline | 2 |
| 145 | 1.3. Federation Use Cases | 3 |
| 146 | 1.3.1. Federation Considerations | 3 |
| 147 | 1.4. Audience | 5 |
| 148 | 1.5. Notations | 5 |
| 149 | 1.6. Document Structure | 5 |
| 150 | 2. Architecture | 7 |
| 151 | 2.1. PIV Identity Account | 8 |
| 152 | 2.1.1. PIV Credentials | 9 |
| 153 | 2.1.2. Home Agency Identity Management System | 9 |
| 154 | 2.2. Identity Providers | 9 |
| 155 | 2.2.1. PIV IdP | 10 |
| 156 | 2.2.2. Home Agency IdP | 11 |
| 157 | 2.2.3. Subscriber-Controlled wallets | 12 |
| 158 | 2.3. Relying Parties | 12 |
| 159 | 3. Trust Agreements | 13 |
| 160 | 3.1. Bilateral Agreements | 15 |
| 161 | 3.2. Multilateral Agreements | 15 |
| 162 | 3.3. Identity Proxies and Brokers | 16 |
| 163 | 3.4. Shared Signaling | 17 |
| 164 | 3.5. Home Agency IdPs | 18 |
| 165 | 3.5.1. Home Agencies and Subscriber-Controlled Wallet | 19 |
| 166 | 4. Federation Assurance Level (FAL) | 20 |
| 167 | 4.1. Reaching Different FALs in PIV Federation | 20 |
| 168 | 4.1.1. FAL1 | 20 |
| 169 | 4.1.2. FAL2 | 20 |
| 170 | 4.1.3. FAL3 | 21 |
| 171 | 4.2. Selecting FAL | 23 |

| | | |
|-----|-----------------------------------------------------------------|----|
| 172 | 5. Requirements of IdPs and RPs | 24 |
| 173 | 5.1. General-Purpose IdP Requirements | 24 |
| 174 | 5.1.1. Authentication Requirements | 24 |
| 175 | 5.1.2. PIV Identity Account Identification | 25 |
| 176 | 5.1.3. Session Management | 25 |
| 177 | 5.2. Subscriber-Controlled wallets | 26 |
| 178 | 5.3. RP Requirements | 26 |
| 179 | 5.3.1. Assertion Processing | 26 |
| 180 | 5.3.2. RP Subscriber Accounts | 26 |
| 181 | 5.3.3. Session Management | 27 |
| 182 | 5.3.4. Changing the Federated Identifier | 27 |
| 183 | 6. Protocol Requirements | 28 |
| 184 | 6.1. Required Attributes | 28 |
| 185 | 6.1.1. Last Updated Time | 29 |
| 186 | 6.2. Assertion Contents | 30 |
| 187 | 6.2.1. Federated Identifier | 31 |
| 188 | 6.2.2. Authorization and Access Rights | 32 |
| 189 | 6.2.3. Certificate Identifiers | 32 |
| 190 | 6.3. Discovery and Registration | 32 |
| 191 | 6.4. Assertion Presentation | 33 |
| 192 | 6.5. Attribute APIs | 33 |
| 193 | 6.6. Identity Proxies and Brokers | 33 |
| 194 | References | 34 |
| 195 | Appendix A. Examples | 35 |
| 196 | A.1. Direct Connection to the Home Agency IdP | 35 |
| 197 | A.2. Multilateral Federation Network | 35 |
| 198 | A.3. Enterprise Application | 36 |
| 199 | A.4. PKI-Based Federation Gateway | 37 |
| 200 | A.5. PIV Federation Proxy as a Federation Authority | 37 |
| 201 | A.6. FAL3 With a PIV Card and PKI-Based Derived PIV Credentials | 38 |
| 202 | A.7. FAL3 With an RP-Bound Authenticator | 38 |
| 203 | A.8. Issuance to a Digital Wallet | 38 |

| | | |
|-----|----------------------------------------------------|----|
| 204 | Appendix B. Glossary of Terms | 40 |
| 205 | Appendix C. Abbreviations | 41 |
| 206 | List of Tables | |
| 207 | List of Figures | |
| 208 | Fig. 1. PIV Federation | 7 |
| 209 | Fig. 2. IdP-managed bound authenticators | 22 |
| 210 | Fig. 3. RP-managed bound authenticators | 22 |

211 **1. Introduction**

212 *This section is informative.*

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

223 **1.1. Background**

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

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

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

240 **1.2. Purpose and Scope**

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

249 **1.2.1. Creating Technical Interoperability Profiles of This Guideline**

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

256 **Target Protocols:**

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

261 **Attribute Naming:**

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

267 **Attribute Contents:**

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

273 **Conformance Criteria:**

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

279 **Home Agency IdP Records:**

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

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

286 **1.3. Federation Use Cases**

287 In a *direct authentication*, the claimant presents their authenticator to a verifier, which is
288 tightly coupled with the RP and, usually, the home agency IdMS described in [Sec 2.1.2](#).

289 The verifier conducts an authentication process of a PIV credential. This process
290 sometimes uses an external service, such as when public key infrastructure is used to
291 validate a certificate.

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

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

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

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

317 **1.3.1. Federation Considerations**

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

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

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

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

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

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

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

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

365 **1.4. Audience**

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

369 **1.5. Notations**

370 This guideline uses the following typographical conventions in text:

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

386 **1.6. Document Structure**

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

- 389 • Section 2 describes a general architecture for PIV federation. This section is
390 *informative*.
- 391 • Section 3 describes the trust agreements in a PIV federation. This section is
392 *normative*.
- 393 • Section 4 describes the Federation Assurance Levels as applied to PIV federation.
394 This section is *normative*.
- 395 • Section 5 describes the requirements for IdPs and RPs in a PIV federation. This
396 section is *normative*.
- 397 • Section 6 describes the requirements for protocol elements in a PIV federation,
398 including assertion contents. This section is *normative*.

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

405 **2. Architecture**

406 *This section is informative.*

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

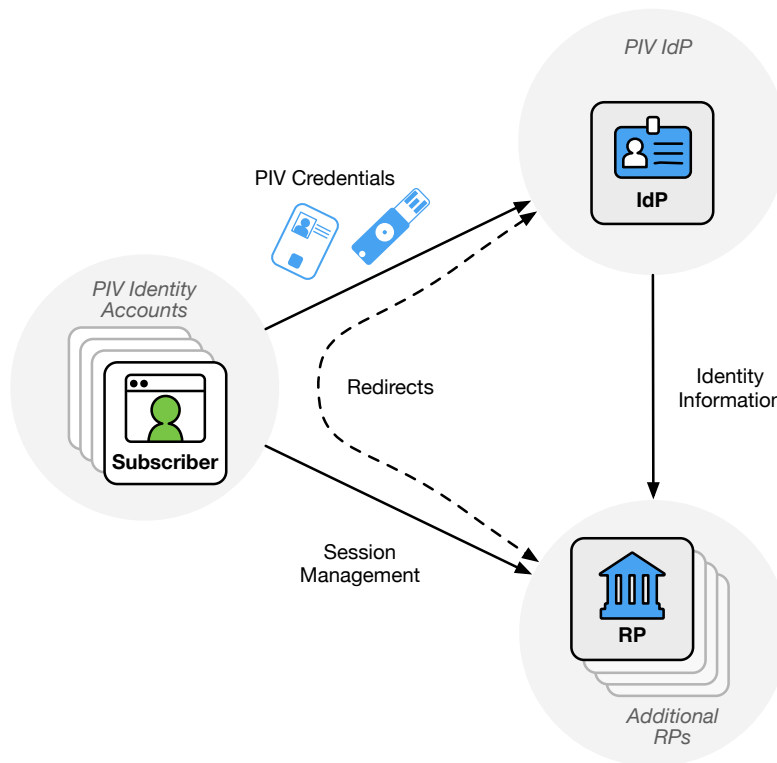


Fig. 1. PIV Federation

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

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

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

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

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

435 **2.1. PIV Identity Account**

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

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

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

451 **2.1.1. PIV Credentials**

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

460 **2.1.2. Home Agency Identity Management System**

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

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

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

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

483 **2.2. Identity Providers**

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

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

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

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

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

520 **2.2.1. PIV IdP**

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

524 The population of PIV identity accounts served by a given PIV IdP can be determined
525 based on a variety of factors but is usually based on the home agency of the PIV identity
526 account. That is to say, an trust agreement will indicate that an agency's PIV identity

527 accounts will be served by one specific IdP. Within any trust agreement, the RP needs
528 to know which IdP to accept assertions about a particular PIV identity account from.

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

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

537 **2.2.2. Home Agency IdP**

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

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

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

552 **2.2.3. Subscriber-Controlled wallets**

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

558 **2.3. Relying Parties**

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

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

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

574 **3. Trust Agreements**

575 *This section is normative.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

648 **3.1. Bilateral Agreements**

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

651 When the PIV IdP is the home agency IdP for an agency, the home agency IdMS **SHALL**
652 make its home agency IdP record available to the connected RP, as described in [Sec. 3.5](#).
653 The RP operator **SHALL** make the information in the home agency IdP record available to
654 authenticated subscribers from that IdP upon request.

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

657 **3.2. Multilateral Agreements**

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

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

672 The federation authority **SHALL** disclose to all connected RPs whether a particular
673 IdP is the home agency IdP for a subscriber population. Federation authorities **SHALL**

674 make all home agency IdP records (defined in [Sec. 3.5](#)) available to participants within
675 the federation using a machine-readable format that is appropriate for the federation
676 protocol standards in use. The federation authority **MAY** provide the home agency IdP
677 records directly or through a pointer to a resource hosted by the home agency. As part
678 of the trust agreement, the home agency **SHALL** document that its home agency IdP
679 record is available through the federation authority in question.

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

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

689 **3.3. Identity Proxies and Brokers**

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

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

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

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

710 Assertions created by a proxy **SHALL** include the identifier of the upstream IdP. This
711 is separate from the required issuer field, which identifies the proxy itself. Since the

712 proxy is the issuer of federated assertions to its downstream RPs, these downstream RPs
713 **SHALL** view the proxy as the PIV IdP for accounts asserted through the proxy.

714 **3.4. Shared Signaling**

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

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

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

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

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

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

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

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

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

738 **3.5. Home Agency IdPs**

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

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

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

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

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

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

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

769 **3.5.1. Home Agencies and Subscriber-Controlled Wallet**

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

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

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

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

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

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

789 *This section is normative.*

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

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

799 **4.1. Reaching Different FALs in PIV Federation**

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

804 **4.1.1. FAL1**

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

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

815 **4.1.2. FAL2**

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

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

821 The establishment of the trust agreement and determination of the PIV IdP at
822 FAL2 **SHALL** be performed prior to the start of the federation transaction. In this

823 establishment, the RP **SHALL** ensure that the PIV IdP is the home agency IdP that
824 represents the population of accounts in question. This process **MAY** be augmented
825 by automated processes (e.g., key exchange) and facilitated by trusted parties (e.g.,
826 federation authority).

827 **4.1.3. FAL3**

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

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

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

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

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

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

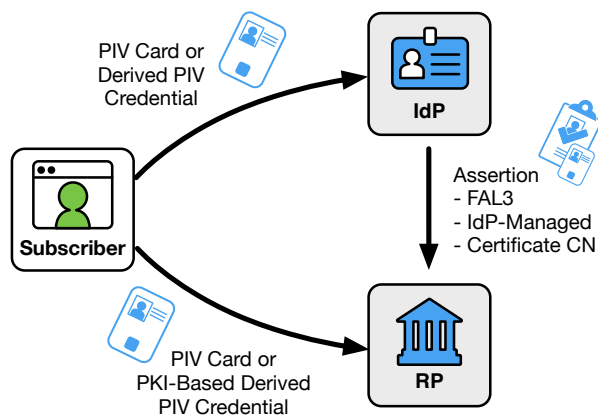


Fig. 2. IdP-managed bound authenticators

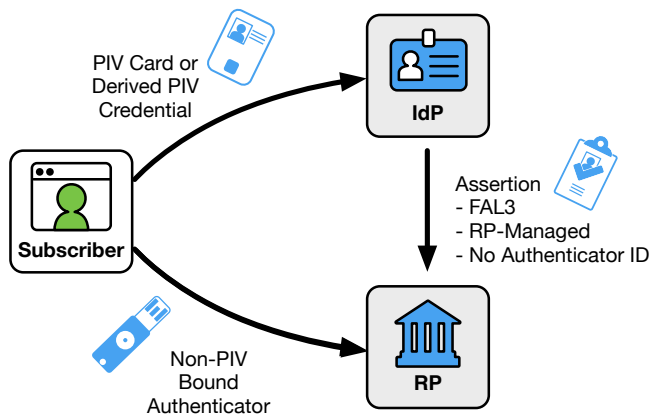


Fig. 3. RP-managed bound authenticators

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

863 **4.2. Selecting FAL**

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

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

876 **5. Requirements of IdPs and RPs**

877 *This section is normative.*

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

879 **5.1. General-Purpose IdP Requirements**

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

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

885 **5.1.1. Authentication Requirements**

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

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

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

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

907 Note: for PIV IdPs using PKI-based PIV credentials as the only authenticators, the active
908 status of the PIV identity account could be partially inferred from the validity of the
909 certificate used for authentication. As long as revocation and expiration checks of
910 the certificate are processed, a valid certificate is likely to indicate a valid PIV identity

911 account. However, the certificate status does not necessarily reflect the status of the
912 associated PIV identity account. A PIV certificate could be expired or revoked due to
913 compromise for a cardholder whose PIV identity account remains in good standing.
914 Additionally, the status of a certificate from a terminated PIV identity account may not
915 be immediately reflected in the associated certificate revocation list, as Section 2.9.1 of
916 [FIPS201] allows for 18 hours to complete the revocation process.

917 **5.1.2. PIV Identity Account Identification**

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

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

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

929 **5.1.3. Session Management**

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

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

937 **5.2. Subscriber-Controlled wallets**

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

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

948 **5.3. RP Requirements**

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

950 **5.3.1. Assertion Processing**

951 The RP **SHALL** verify that all assertions contain all required elements as enumerated in
952 [Sec. 6.2](#). The RP **SHALL** reject any assertion that does not meet these requirements.

953 **5.3.2. RP Subscriber Accounts**

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

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

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

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

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

973 **5.3.3. Session Management**

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

978 The RP **SHALL** follow all session management requirements for RPs defined in
979 [\[SP800-63C\]](#).

980 **5.3.4. Changing the Federated Identifier**

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

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

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

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

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

996 **6. Protocol Requirements**

997 *This section is normative.*

998 A federation protocol connects the IdP and RP together with a series of messages.
999 These messages include assertions, which are passed between the IdP and RP to
1000 represent the federated authentication event, and the contents of identity APIs, which
1001 convey additional attribute information about the subscriber. This section enumerates
1002 requirements for these common components but is not intended to provide sufficient
1003 detail for any specific federation protocol.

1004 **6.1. Required Attributes**

1005 As stated in [Sec. 3](#), the trust agreement establishes the set of attributes that the IdP
1006 provides to the RP and the purposes the RP has for those attributes. Some attributes
1007 are required to be available at the IdP. Some of the available attributes are mandatory
1008 to be provided to all RPs. Other attributes are available at the IdP but accessible only
1009 to RPs if stipulated in the trust agreement. Other attributes are optional for the IdP
1010 to have available, and likewise optional to be provided to RPs if stipulated in the trust
1011 agreement. The identity attributes found in the PIV identity account that are made
1012 available from a PIV IdP are not limited to those available from the PIV authentication
1013 certificate.

1014 The following set of identity attributes **SHALL** be provided by a PIV IdP to every RP within
1015 any trust agreement for PIV federation:

- 1016 • **Subject Identifier:** A unique identifier for the PIV identity account that is assigned
1017 by the IdP to the account for use by the RP. The subject identifier is part of the
1018 federated identifier (see [Sec. 6.2.1](#) for additional requirements).
- 1019 • **Home Agency:** A global identifier for the home agency associated with the PIV
1020 identity account (e.g., an agency's domain name or a FASC-N agency code from
1021 [\[SP800-87\]](#)).
- 1022 • **Organizational Affiliation:** The organization or list of organizations with which the
1023 PIV identity account is affiliated using global identifiers for the organization (e.g.,
1024 an agency's domain name or a FASC-N agency code from [\[SP800-87\]](#)). This can
1025 be the same as the home agency but may be different in practice. For example,
1026 an employee's home agency may be the parent organization but their account is
1027 affiliated with the specific sub-organizations to which they are assigned.
- 1028 • **Last Updated:** A timestamp that indicates when the available attributes in the PIV
1029 identity account were last updated at the IdP. (see [Sec. 6.1.1.](#))

1030 A PIV IdP **SHALL** have the following core identity attributes available as part of the
1031 account and **SHALL** make those attributes available to an RP if stipulated in the trust
1032 agreement:

- 1033 • Full Name: The full name of the subscriber that is suitable for display or addressing
1034 the subscriber at the RP. Individual portions of the name (e.g., a given name or
1035 family name) **MAY** also be made available separately.

1036 A PIV IdP **SHOULD** have the following core identity attributes available as part of the
1037 account and **SHOULD** make those attributes available to an RP if stipulated in the trust
1038 agreement:

- 1039 • Email address: The current email address for the subscriber as known by or issued
1040 by the IdP
- 1041 • Physical Address: The physical address of the subscriber, typically an office address
- 1042 • Phone Number: The current telephone number for the subscriber as known by or
1043 issued by the IdP
- 1044 • Certificate Identifier: The identifier of the PIV authentication certificate (see
1045 [Sec 6.2.3](#))

1046 Except as otherwise stated in [Sec. 6.2](#), the IdP **SHOULD** disclose attributes through an
1047 identity API rather than through the assertion itself. For example, in OpenID Connect,
1048 while it is possible to include subscriber attributes such as `name` and `email` within
1049 the ID token (the assertion), it is preferable to make such attributes available from the
1050 UserInfo Endpoint (an identity API). When attributes are available for a given account
1051 through more than one method at an IdP, the attribute values **SHALL** match.

1052 A PIV IdP **SHOULD** allow for selective disclosure of attributes to different RPs, as
1053 determined by the authorized party listed in the trust agreement.

1054 **6.1.1. Last Updated Time**

1055 The last updated attribute is provided as a hint to the RP about the current freshness
1056 of the attributes available from the IdP to allow the RP to decide when to refresh any
1057 attributes kept in the RP subscriber account.

1058 The timestamp is calculated by the IdP, and its source varies depending on
1059 implementation. For example, for the home agency IdP, this would include any
1060 modifications made to the PIV identity account that affect the attributes that the IdP
1061 makes available. For other PIV IdPs, the last updated timestamp indicates when the
1062 IdP's copies of any attributes were last updated from their source. In all cases, the RP
1063 can track this timestamp as a value stored in the RP subscriber account. If the timestamp
1064 provided by the IdP is newer than that in the RP subscriber account, the RP can update
1065 its cached attributes from the IdP using any available mechanisms.

1066 If multiple timestamps are available for different attributes, the latest timestamp **SHALL**
1067 be used.

1068 **6.2. Assertion Contents**

1069 As specified in [SP800-63C], the successful validation of a federated assertion is required
1070 to begin an authenticated session at the RP. The assertion contains a combination of
1071 attributes about the subscriber as well as attributes about the authentication event that
1072 the assertion represents.

1073 At a minimum, the assertion in PIV federation **SHALL** contain the following attributes of
1074 the PIV identity account:

- 1075 • Flag indicating that this assertion represents a PIV federation transaction
- 1076 • Last updated timestamp for the PIV identity account
- 1077 • Identifier for the home agency of the PIV identity account
- 1078 • IAL for the PIV identity account (note that all PIV identity accounts are established
1079 at IAL3)
- 1080 • Federated identifier for the PIV identity account at this IdP, as defined in [Sec. 6.2.1](#)

1081 As an assertion is a short-lived message from the IdP to the RP, the assertion itself
1082 **SHOULD** only contain the minimum attributes required for its processing. To preserve
1083 privacy and minimize the information sent with each request, the assertion **SHOULD NOT**
1084 contain non-required or stable attributes from the PIV identity account (e.g., email
1085 address, display name). Additional attributes **SHOULD** be made available to the RP
1086 through a standard identity API.

1087 At a minimum, the assertion in PIV federation **SHALL** contain the following attributes of
1088 the authentication event:

- 1089 • AAL for the latest successful authentication event for the subscriber's current
1090 session at the IdP
- 1091 • Timestamp of the latest successful authentication event for the subscriber's
1092 current session at the IdP
- 1093 • Flag indicating whether the PIV Card or a derived PIV credential was used at the
1094 authentication event for the subscriber's current session at the IdP
- 1095 • Intended FAL for the current transaction

1096 For FAL3 assertions in PIV federation, the assertion **SHALL** contain either:

- 1097 • A reference to an IdP-managed bound authenticator to be verified by the RP (e.g.,
1098 a certificate identifier, as discussed in [Sec 6.2.3](#)), or
- 1099 • A flag indicating that an RP-managed bound authenticator is required at the RP.

1100 The mapping of these required attributes to specific fields within a given federation
1101 protocol is out of scope for this specification.

1102 **6.2.1. Federated Identifier**

1103 The assertion created by a PIV IdP includes a *federated identifier* for the PIV identity
1104 account, as defined in [\[SP800-63C\]](#). The federated identifier consists of the logical
1105 combination of both a *subject identifier* for the PIV identity account assigned by the IdP
1106 and a global *issuer identifier* for the IdP.

1107 The subject identifier **SHALL** be unique to the PIV identity account at the IdP such that
1108 no identifier is the same for any two PIV identity accounts at an IdP.

1109 The subject identifier **SHALL** be stable for a PIV identity account over time and **SHALL**
1110 survive common life cycle events, such as reissuance of a PIV Card or changes to
1111 attributes (e.g., email addresses, usernames).

1112 The subject identifier **MAY** be generated by the IdP in a pairwise fashion for a specific
1113 RP, as discussed in [\[SP800-63C\]](#). If such a pairwise identifier is used, it **SHALL** be used
1114 consistently with a given RP and **SHALL NOT** be used for multiple RPs except as allowed
1115 by [\[SP800-63C\]](#).

1116 The subject identifier **SHALL NOT** include any personally identifiable or private
1117 information, such as a username, an certificate identifiers (see [Sec 6.2.3](#)), email
1118 addresses, the UUIDs of the PIV Card or cardholder, or an internal record number. These
1119 identifiers **MAY** be used as input to a one-way cryptographic function used to calculate a
1120 subject identifier. However, care should be taken to ensure that the resulting identifier is
1121 stable.

1122 The issuer identifier **SHALL** be globally unique for the IdP. This identifier is usually the
1123 URL of the IdP, but it can also be a unique key identifier or other globally unique value
1124 that can be verified by the RP as part of the assertion.

1125 The RP **SHALL** use this federated identifier to uniquely associate the PIV identity account
1126 with the RP subscriber account, as defined in [\[SP800-63C\]](#). The RP **SHALL NOT** use other
1127 attributes alone for this purpose, including email addresses, certificate subject names, or
1128 PIV cardholder UUIDs.

1129 **6.2.2. Authorization and Access Rights**

1130 The assertion **MAY** contain indicators for the authorizations and access rights that the
1131 subscriber has at the RP, such as a set of roles within an organization. The RP **SHALL** trust
1132 these only as subject to the details of the trust agreements between the IdP and RP.

1133 As the point of enforcement, the RP **MAY** override these authorizations by additionally
1134 restricting access as necessary.

1135 **6.2.3. Certificate Identifiers**

1136 The PIV authentication certificate is issued to PIV identity cardholders as part of the PIV
1137 Card and can uniquely identify a PIV identity account, as described in [FIPS201]. Within
1138 PIV federation, the PIV authentication certificate is not used for primary authentication
1139 to the RP, but it can still be referred to from the federation protocol in some important
1140 ways. For example, when used as an IdP-managed bound authenticator, the PIV
1141 authentication certificate is verified by both the PIV IdP and subsequently by the RP.
1142 For this to work, the assertion needs to communicate the identity of the certificate
1143 and its included keys in a reliable manner. The exact method of referring to the PIV
1144 authentication certificate is out of scope for this document and subject to profiling of
1145 the federation technology in use, but some common options include:

- 1146 • The cryptographic hash of the public key used in the PIV authentication certificate,
- 1147 • Certificate issuer (CA) and subject identifier
- 1148 • CA and certificate serial number
- 1149 • Subject key identifier
- 1150 • The cryptographic hash of the full certificate
- 1151 • The full certificate value

1152 Each of these options has different tradeoffs and considerations, and an interoperable
1153 technical profile of this specification **SHOULD** define which of these are supported.

1154 **6.3. Discovery and Registration**

1155 The IdP **SHALL** publish its configuration information in a standard machine-readable
1156 format and location that are appropriate to the federation protocol in use. The
1157 information in the configuration document **SHALL** be sufficient to allow for the
1158 automated configuration of an RP contacting the IdP even when the RP is statically
1159 registered.

1160 IdPs operating at FAL2 and below **SHOULD** allow RPs to register dynamically, as described
1161 in [SP800-63C]. Assertions issued to dynamically registered RPs **SHALL** contain pairwise
1162 subject identifiers.

1163 **6.4. Assertion Presentation**

1164 The IdP **SHALL** support back-channel assertion presentation, if possible within
1165 the federation protocol. All back-channel presentation methods **SHALL** require
1166 authentication of the RP.

1167 At all FALs, RPs **SHOULD** use back-channel presentation to fetch the assertion directly
1168 from the IdP, where available.

1169 If front-channel presentation is used and the assertion contains PII, the contents of the
1170 assertion **SHALL** be encrypted using a key specific to the RP, as required in [SP800-63C].

1171 **6.5. Attribute APIs**

1172 The IdP **SHALL** make identity attributes for the subscriber available through a standard
1173 identity API, if possible within the federation protocol in use. The identity API **SHALL**
1174 require protected access from the RP.

1175 The IdP **SHALL** allow limited disclosure of attributes through this API, such that
1176 federation agreements that connect the IdP and RP (including runtime decisions by an
1177 authorized party) can dictate which attributes are disclosed to the RP for a given request.

1178 The RP **SHALL** use the account update timestamp to manage its cache of attribute
1179 information in the RP subscriber account, particularly when using a just-in-time
1180 provisioning model. That is, if the account update timestamp in the assertion is later
1181 than the last cache update value, the RP knows that it should fetch updated information
1182 from the identity API. If the timestamp is not later than the cache time, the RP can
1183 determine that an additional call to the identity API would be redundant.

1184 The IdP **MAY** provide a provisioning API to the RP, subject to a trust agreement. When
1185 a provisioning API is used, the trust agreement **SHALL** include a justification for the
1186 intended use of all attributes provided to the RP by the provisioning API.

1187 **6.6. Identity Proxies and Brokers**

1188 An identity proxy acting in a PIV federation context **SHALL** disclose the IdPs used as
1189 sources of attributes to the downstream RP. For example, if an assertion contains
1190 attributes for a PIV identity account from IdP A and IdP B, the proxy will list both IdPs
1191 as sources within the assertion. Note that the proxy, in its role as an IdP to downstream
1192 RPs, is still the issuer of the assertion and will identify itself as such.

1193 See [Sec. 3.3](#) for more information about the trust agreement requirements of identity
1194 proxies.

1195 **References**

1196 **[FIPS201]** National Institute of Standards and Technology (2022) *Personal Identity*
1197 *Verification (PIV) of Federal Employees and Contractors*. (U.S. Department of Commerce,
1198 Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-3 [or
1199 as amended]. <https://doi.org/10.6028/NIST.FIPS.201-3>

1200 **[SP800-63]** Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle
1201 C, Lefkowitz N, Regenscheid A (2024) *Digital Identity Guidelines*. (National Institute of
1202 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4
1203 2pd, 2024 [or as amended]. <https://doi.org/10.6028/NIST.SP.800-63-4.2pd>

1204 **[SP800-63B]** Temoshok D, Fenton JL, Choong YY, Lefkowitz N, Regenscheid A, Richer
1205 JP (2024) *Digital Identity Guidelines: Authentication and Authenticator Management*.
1206 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
1207 Publication (SP) 800-63B-4 2pd, 2024 [or as amended]. <https://doi.org/10.6028/NIST.SP.800-63b-4.2pd>

1209 **[SP800-63C]** Temoshok D, Richer JP, Choong YY, Fenton JL, Lefkowitz N, Regenscheid
1210 A (2024) *Digital Identity Guidelines: Federation and Assertions*. (National Institute of
1211 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63C-4
1212 2pd, 2024 [or as amended]. <https://doi.org/10.6028/NIST.SP.800-63c-4.2pd>

1213 **[SP800-87]** Ferraiolo H (2018) *Codes for the Identification of Federal and Federally-*
1214 *Assisted Organizations*, (National Institute of Standards and Technology, Gaithersburg,
1215 MD), NIST Special Publication (SP) 800-87r2 [or as amended]. [https://doi.org/10.6028/](https://doi.org/10.6028/NIST.SP.800-87r2)
1216 [NIST.SP.800-87r2](https://doi.org/10.6028/NIST.SP.800-87r2)

1217 **[SP800-157]** Ferraiolo H, Regenscheid AR, Fenton J (2024) *Guidelines for Derived*
1218 *Personal Identity Verification (PIV) Credentials*. (National Institute of Standards and
1219 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-157 Revision 1 [or as
1220 amended]. <https://doi.org/10.6028/NIST.SP.800-157r1-fpd>

1221 **Appendix A. Examples**

1222 *This appendix is informative.*

1223 This appendix contains several example scenarios of PIV federation in various
1224 environments and applications to show different kinds of trust establishment, account
1225 management, and authenticator usage. The details of the federation transactions within
1226 each scenario all follow the common patterns discussed in [SP800-63C] and adhere to
1227 the requirements in this document.

1228 The scenarios in this section are for illustrative purposes and do not convey additional
1229 requirements beyond those imposed by this specification.

1230 **A.1. Direct Connection to the Home Agency IdP**

1231 Agency A, which issues and manages PIV identity accounts, sets up an OpenID Connect
1232 IdP in order to make its PIV identity accounts available online through a federation
1233 process. The agency publishes its home agency IdP record from its publicly available
1234 website with all of the information required by RPs to establish a connection.

1235 The RP enters into a pairwise trust agreement with the IdP to accept assertions for
1236 Agency A. The RP declares the set of attributes that it needs from the IdP as part of
1237 this agreement. The RP uses a just-in-time provisioning system to establish an RP
1238 subscriber account when the subscriber logs in for the first time. The RP has other
1239 pairwise agreements with other IdPs to accept assertions for different agencies but will
1240 reject any assertions for accounts at Agency A that come from any other IdP.

1241 The IdP generates a pairwise federated identifier for the PIV identity account for each
1242 RP that it is in contact with by hashing the identifier for the RP along with a randomly
1243 generated value stored with the PIV identity account at the IdP. This way, each new RP
1244 that signs on to the IdP gets a different federated identifier for a single account, but a
1245 consistent federated identifier is used for each RP with that account.

1246 Per the terms of the trust agreement, the subscriber is prompted by the IdP the first
1247 time they log on to the RP. The IdP asks for the subscriber's consent at runtime to share
1248 attributes with the RP. The IdP prompts the subscriber to allow the IdP to remember
1249 this consent decision. This stored decision causes the IdP to act on the stored consent
1250 in a future request and not prompt the subscriber if the same RP requests the same
1251 attributes.

1252 **A.2. Multilateral Federation Network**

1253 Agencies A, B, and C each have a home agency IdP running OpenID Connect for their
1254 PIV identity accounts. All three agencies join a multilateral federation in which the
1255 federation authority independently verifies that each home agency IdP represents the
1256 agency in question. The federation authority publishes the home agency IdP records

1257 for all agencies that are part of the multilateral federation. This publication allows RPs
1258 within the federation to discover which IdP is to be used to access accounts for a given
1259 agency under the rules of the federation agreement.

1260 RPs X and Y wish to allow logins from agencies A, B, and C, and the RPs declare their
1261 intent and a list of required attributes to the federation authority. The federation
1262 authority assesses both RP requests and adds them to the multilateral federation. This
1263 allows both RPs to register at each of the three separate IdPs as needed for each agency.

1264 Both RPs interface directly with each of the three IdPs and not through a federation
1265 proxy. When a new IdP or RP is added to the multilateral federation agreement, the
1266 existing IdPs and RPs are notified of the new component and its parameters.

1267 The IdPs and RPs establish a shared signaling channel under the auspices of the
1268 federation authority. This allows any IdP and any RP to report suspicious or malicious
1269 behavior that involves a specific account to the rest of the members under the
1270 federation authority.

1271 **A.3. Enterprise Application**

1272 The home agency IdP establishes a pairwise agreement with an RP to provide an
1273 enterprise-class service to the subjects of the agency's PIV identity accounts. As part
1274 of this trust agreement, the home agency IdP allows access to a provisioning API for the
1275 RP. The provisioning API pushes a set of federated identifiers and associated attributes
1276 to the RP that allow the RP to pre-provision RP subscriber accounts for every PIV identity
1277 account at the IdP.

1278 The existence of these RP subscriber accounts allows the RP to offer things like access
1279 rights, sharing, and messaging to all accounts on the system, whether or not the specific
1280 account has logged in to the RP yet.

1281 Under the terms of the trust agreement, the RP is placed on an allowlist. Consequently,
1282 subscribers are not prompted for consent at runtime because the agency consented to
1283 use the service on behalf of all accounts at the time the RP was onboarded. This gives
1284 subscribers a seamless single sign-on experience, even though a federation protocol
1285 is being used across security domain boundaries. The RP can always request a re-
1286 authentication of the subscriber, resulting in a fresh assertion from the IdP.

1287 The RP subscriber accounts are synchronized using the provisioning API. When a new
1288 PIV identity account is created, modified, or deleted at the IdP, the IdP updates the
1289 status of the RP subscriber account using the provisioning API. This allows the RP to
1290 always have an up-to-date status for each PIV identity account. For example, when the
1291 subscriber account is terminated at the IdP, the provisioning API signals to the RP that
1292 the RP subscriber account is to be terminated immediately. The RP removes all locally
1293 cached attributes for the account in question, except for the identifiers and references in
1294 audit and access logs.

1295 **A.4. PKI-Based Federation Gateway**

1296 A service provider that does not issue any PIV identity account of its own sets up a SAML
1297 IdP that accepts PKI-based PIV credentials as its only authentication method. These
1298 accounts are provisioned at the IdP using the attributes in the certificates when the
1299 subscriber first presents the certificate. The IdP collects no additional attributes from
1300 the subscriber in the process.

1301 The IdP generates federated identifiers for the accounts by computing a hash of the
1302 authentication certificate and encoding that hash in Base64. This process fulfills the
1303 requirements of this document for federated identifiers, but it is specific to this IdP
1304 and need not be known or understood by any RP connecting through the IdP. If the
1305 subscriber changes any attributes in the certificate (e.g., their name), then a new
1306 federated identifier will be created as a result. As a result, this IdP does not necessarily
1307 provide a stable subject identifier across authenticator updates.

1308 The RP enters into a pairwise trust agreement with the IdP to accept assertions for
1309 any agency with PIV credentials. The RP does not have any other IdPs that it speaks to
1310 directly, and so the only way to log in to the RP is through this gateway. Since the IdP
1311 accepts a broad range of PKI-based credentials, this allows the RP access to any account
1312 based on those credentials.

1313 This setup does not allow the PIV identity accounts to use non-PKI-based derived PIV
1314 credentials since the IdP portion of the gateway is not the home agency IdP for any of
1315 the accounts in question. The RP is also not able to receive any attributes other than
1316 those available directly to the IdP through subscriber certificates. To ensure account
1317 continuity, an RP would need to have an out-of-band process to bind their new federated
1318 identifier to the existing RP subscriber account if the certificate and attributes change
1319 over time.

1320 The IdP is not acting as a federation proxy because the inbound credential is not a
1321 federated assertion but rather a PKI-based credential that the gateway processes directly
1322 as a verifier.

1323 **A.5. PIV Federation Proxy as a Federation Authority**

1324 A federation proxy is set up within a multilateral federation. The proxy is run by the
1325 federation authority. All IdPs under the multilateral agreement register the proxy as an
1326 RP. The RPs within the federation authority connect to the proxy as their only IdP. All
1327 federation transactions within the multilateral federation flow through the proxy.

1328 The federation authority discloses the nature of the proxy to all parties, so the IdPs know
1329 that this particular RP is a proxy, and the RPs know that their IdP is a proxy. Furthermore,
1330 the proxy lists all of the upstream IdPs and their associated populations of PIV identity
1331 accounts to all RPs connecting through the proxy.

1332 The proxy discloses to the RPs which upstream IdPs participated in the authentication of
1333 the PIV identity account to the proxy, allowing the downstream RPs to validate that the
1334 source of the federation transaction through the proxy is appropriate for the PIV identity
1335 account in question.

1336 The proxy is not regarded as a home agency IdP for any RP in the system, even if the IdPs
1337 connecting to the proxy are themselves home agency IdPs.

1338 **A.6. FAL3 With a PIV Card and PKI-Based Derived PIV Credentials**

1339 The PIV Card and certain PKI-based derived PIV credentials can be used as IdP-managed
1340 bound authenticators for use at FAL3. The home agency IdP authenticates the PIV
1341 identity account using an authenticator bound to the account and then creates an
1342 assertion that is flagged as FAL3. The assertion also contains the certificate common
1343 name (CN) and thumbprint of the certificate to be used as a bound authenticator.

1344 When the RP receives the assertion, it processes it as usual and sees the FAL3 flag and
1345 the certificate attributes. The RP matches the CN against attributes in the RP Subscriber
1346 Account to ensure that the certificate being identified is appropriate for the PIV identity
1347 account being represented. The RP then prompts the subscriber to authenticate using
1348 a certificate and compares that certificate against the provided CN and thumbprint,
1349 ensuring that they match. When the certificate has been validated, the RP creates a
1350 secure session at FAL3. From this point forward in the session, the RP no longer requires
1351 presentation of the certificate in order to access the RP's services.

1352 **A.7. FAL3 With an RP-Bound Authenticator**

1353 The home agency IdP authenticates the PIV identity account using an authenticator
1354 bound to the account, and then creates an assertion that is flagged as FAL3 and using
1355 an RP-bound authenticator.

1356 When the RP receives the assertion, it processes it as usual and sees the FAL3 flag. The
1357 RP looks up the bound authenticator associated with the RP Subscriber Account and
1358 prompts the subscriber for this authenticator. When the authenticator has been verified,
1359 the RP creates a secure session at FAL3.

1360 **A.8. Issuance to a Digital Wallet**

1361 The home agency provides a service to issue PIV-account-backed credentials to digital
1362 wallets. This home agency has decided to accept any wallet as capable of issuing
1363 credentials at FAL1. During issuance, the subscriber logs in to the home agency's issuing
1364 endpoint using their PIV Card. The subscriber activates their wallet and presents it to the
1365 home agency, which issues a signed attribute bundle to the wallet representing the PIV
1366 identity account.

1367 During the federated transaction, the subscriber presents their wallet to the RP to log in.
1368 The RP requests an assertion from the wallet, which is acting as the IdP. The subscriber
1369 activates the wallet, and the wallet issues an assertion and delivers it to the RP. The
1370 RP looks up the home agency's attribute bundle signing keys and validates the signed
1371 attribute bundle based on those keys. The RP then validates the assertion based on the
1372 key included in the signed attribute bundle.

1373 **Appendix B. Glossary of Terms**

1374 *This section is informative.*

1375 **home agency**

1376 The agency responsible for the issuance and management of a PIV identity account. Also
1377 known as the issuing agency, with regard to the PIV identity account.

1378 **home agency identity management system (IdMS)**

1379 The identity management system that stores and manages the PIV identity account, its
1380 associated attributes, and PIV credential bindings.

1381 **home agency identity provider (IdP)**

1382 The officially sanctioned identity provider of the home agency for a PIV identity account.

1383 **identity provider (IdP)**

1384 The party that verifies the credentials of a subscriber account and issues assertions to an
1385 RP based on that account for federation.

1386 **organizational affiliation**

1387 The list of organizations affiliated with a PIV identity account. This is often the same as
1388 the home agency, but can be different in practice.

1389 **PIV credential**

1390 A PIV Card or derived PIV credential.

1391 **PIV federation**

1392 A federation process that presents a PIV identity account from a PIV IdP. The subscriber is
1393 authenticated at the IdP using PIV credentials.

1394 **PIV identity provider (IdP)**

1395 An identity provider that accepts PIV credentials as authenticators for PIV identity
1396 accounts as part of PIV federation. The IdP trusted by the RP to create assertions for a
1397 PIV identity account.

1398 **relying party (RP)**

1399 The party that accepts an assertion from an IdP to allow the federated login of a PIV
1400 identity account.

1401 **Appendix C. Abbreviations**

1402 *This section is informative.*

1403 **AAL**

1404 Authentication Assurance Level

1405 **API**

1406 Application Programming Interface

1407 **CSP**

1408 Credential Service Provider

1409 **FAL**

1410 Federation Assurance Level

1411 **FASC-N**

1412 Federal Agency Smart Credential Number

1413 **IAL**

1414 Identity Assurance Level

1415 **IdP**

1416 Identity Provider

1417 **IdMS**

1418 Identity Management System

1419 **PKI**

1420 Public Key Infrastructure

1421 **PIV**

1422 Personal Identity Verification

1423 **RP**

1424 Relying Party