



1

NIST Special Publication NIST SP 800-63-4 ipd

2

3

Digital Identity Guidelines

4

Initial Public Draft

5

David Temoshok

6

Diana Proud-Madruga

7

Yee-Yin Choong

8

Ryan Galluzzo

9

Sarbari Gupta

10

Connie LaSalle

11

Naomi Lefkowitz

12

Andrew Regenscheid

13

This publication is available free of charge from:

14

<https://doi.org/10.6028/NIST.SP.800-63-4.ipd>

15



16 NIST Special Publication
17 NIST SP 800-63-4 ipd
18 Digital Identity Guidelines
19 Initial Public Draft

20 David Temoshok
21 Ryan Galluzzo
22 Connie LaSalle
23 Naomi Lefkovitz
24 *Applied Cybersecurity Division*
25 *Information Technology Laboratory*

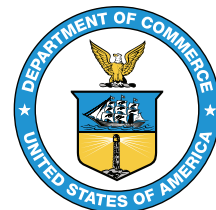
26 Andrew Regenscheid
27 *Computer Security Division*
28 *Information Technology Laboratory*

29 Yee-Yin Choong
30 *Information Access Division*
31 *Information Technology Laboratory*

32 Diana Proud-Madruga
33 Sarbari Gupta
34 *Electrosoft*

35 This publication is available free of charge from:
36 <https://doi.org/10.6028/NIST.SP.800-63-4.ipd>

37 December 2022



39 U.S. Department of Commerce
40 *Gina M. Raimondo, Secretary*

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

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

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

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

58 **Authority**

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

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

74 **NIST Technical Series Policies**

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

77 **Publication History**

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

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

81 Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle C, Lefkovitz
82 N, Regenscheid A (2022) Digital Identity Guidelines. (National Institute of Standards and
83 Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-4 ipd.
84 <https://doi.org/10.6028/NIST.SP.800-63-4.ipd>

85 **Author ORCID iDs**

86 David Temoshok: 0000-0001-6195-0331
87 Diana Proud-Madruga: 0000-0002-8972-7809
88 Yee-Yin Choong: 0000-0002-3889-6047
89 Ryan Galluzzo: 0000-0003-0304-4239
90 Sarbari Gupta: 0000-0003-1101-0856
91 Connie LaSalle: 0000-0001-6031-7550
92 Naomi Lefkovitz: 0000-0003-3777-3106
93 Andrew Regenscheid: 0000-0002-3930-527X

94 **Public Comment Period**

95 December 16, 2022 - March 24, 2023

96 **Submit Comments**

97 <mailto:dig-comments@nist.gov>

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

100 **Reports on Computer Systems Technology**

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

112 **Abstract**

113 These guidelines provide technical requirements for federal agencies implementing digital
114 identity services and are not intended to constrain the development or use of standards
115 outside of this purpose. The guidelines cover identity proofing and authentication of users
116 (such as employees, contractors, or private individuals) interacting with government
117 information systems over networks. They define technical requirements in each of
118 the areas of identity proofing, registration, authenticators, management processes,
119 authentication protocols, federation, and related assertions. This publication will
120 supersede NIST Special Publication 800-63-3.

121 **Keywords**

122 authentication; authentication assurance; authenticator; assertions; credential service
123 provider; digital authentication; digital credentials; identity proofing; federation;
124 passwords; PKI.

125 **Note to Reviewers**

126 The rapid proliferation of online services over the past few years has heightened the need
127 for reliable, equitable, secure, and privacy-protective digital identity solutions.

128 Revision 4 of NIST Special Publication 800-63, Digital Identity Guidelines, intends to
129 respond to the changing digital landscape that has emerged since the last major revision
130 of this suite was published in 2017 — including the real-world implications of online
131 risks. The guidelines present the process and technical requirements for meeting digital
132 identity management assurance levels for identity proofing, authentication, and federation,
133 including requirements for security and privacy as well as considerations for fostering
134 equity and the usability of digital identity solutions and technology.

135 Taking into account feedback provided in response to our [June 2020 Pre-Draft Call](#)
136 [for Comments](#), as well as research conducted into real-world implementations of the
137 guidelines, market innovation, and the current threat environment, this draft seeks to:

- 138 1. **Advance Equity:** This draft seeks to expand upon the risk management content
139 of previous revisions and specifically mandates that agencies account for impacts
140 to individuals and communities in addition to impacts to the organization. It also
141 elevates risks to mission delivery – including challenges to providing services to
142 all people who are eligible for and entitled to them – within the risk management
143 process and when implementing digital identity systems. Additionally, the guidance
144 now mandates continuous evaluation of potential impacts across demographics,
145 provides biometric performance requirements, and additional parameters for the
146 responsible use of biometric-based technologies, such as those that utilize face
147 recognition.
- 148 2. **Emphasize Optionality and Choice for Consumers:** In the interest of promoting
149 and investigating additional scalable, equitable, and convenient identify verification
150 options, including those that do and do not leverage face recognition technologies,
151 this draft expands the list of acceptable identity proofing alternatives to provide
152 new mechanisms to securely deliver services to individuals with differing means,
153 motivations, and backgrounds. The revision also emphasizes the need for digital
154 identity services to support multiple authenticator options to address diverse
155 consumer needs and secure account recovery.
- 156 3. **Deter Fraud and Advanced Threats:** This draft enhances fraud prevention
157 measures from the third revision by updating risk and threat models to account
158 for new attacks, providing new options for phishing resistant authentication, and
159 introducing requirements to prevent automated attacks against enrollment processes.
160 It also opens the door to new technology such as mobile driver’s licenses and
161 verifiable credentials.
- 162 4. **Address Implementation Lessons Learned:** This draft addresses areas where
163 implementation experience has indicated that additional clarity or detail was
164 required to effectively operationalize the guidelines. This includes re-working
165 the federation assurance levels, providing greater detail on Trusted Referees,
166 clarifying guidelines on identity attribute validation sources, and improving address
167 confirmation requirements.

168 NIST is specifically interested in comments on and recommendations for the following
169 topics:

170 **Identity Proofing and Enrollment**

- 171 • NIST sees a need for inclusion of an unattended, fully remote Identity Assurance
172 Level (IAL) 2 identity proofing workflow that provides security and convenience,
173 but does not require face recognition. Accordingly, NIST seeks input on the
174 following questions:

- 175 – What technologies or methods can be applied to develop a remote, unattended
176 IAL2 identity proofing process that demonstrably mitigates the same risks as
177 the current IAL2 process?
- 178 – Are these technologies supported by existing or emerging technical standards?
- 179 – Do these technologies have established metrics and testing methodologies to
180 allow for assessment of performance and understanding of impacts across user
181 populations (e.g., bias in artificial intelligence)?
- 182 • What methods exist for integrating digital evidence (e.g., Mobile Driver’s Licenses,
183 Verifiable Credentials) into identity proofing at various identity assurance levels?
- 184 • What are the impacts, benefits, and risks of specifying a set of requirements
185 for CSPs to establish and maintain fraud detection, response, and notification
186 capabilities?
 - 187 – Are there existing fraud checks (e.g., date of death) or fraud prevention
188 techniques (e.g., device fingerprinting) that should be incorporated as baseline
189 normative requirements? If so, at what assurance levels could these be
190 applied?
 - 191 – How might emerging methods such as fraud analytics and risk scoring be
192 further researched, standardized, measured, and integrated into the guidance in
193 the future?
 - 194 – What accompanying privacy and equity considerations should be addressed
195 alongside these methods?
- 196 • Are current testing programs for liveness detection and presentation attack
197 detection sufficient for evaluating the performance of implementations and
198 technologies?
- 199 • What impacts would the proposed biometric performance requirements for identity
200 proofing have on real-world implementations of biometric technologies?

201 **Risk Management**

- 202 • What additional guidance or direction can be provided to integrate digital identity
203 risk with enterprise risk management?
- 204 • How might equity, privacy, and usability impacts be integrated into the assurance
205 level selection process and digital identity risk management model?
- 206 • How might risk analytics and fraud mitigation techniques be integrated into the
207 selection of different identity assurance levels? How can we qualify or quantify
208 their ability to mitigate overall identity risk?

209 **Authentication and Lifecycle Management**

- 210 • Are emerging authentication models and techniques – such as FIDO passkey,
211 Verifiable Credentials, and mobile driver’s licenses – sufficiently addressed and
212 accommodated, as appropriate, by the guidelines? What are the potential associated
213 security, privacy, and usability benefits and risks?
- 214 • Are the controls for phishing resistance as defined in the guidelines for AAL2 and
215 AAL3 authentication clear and sufficient?
- 216 • How are session management thresholds and reauthentication requirements
217 implemented by agencies and organizations? Should NIST provide thresholds or
218 leave session lengths to agencies based on applications, users, and mission needs?
- 219 • What impacts would the proposed biometric performance requirements for this
220 volume have on real-world implementations of biometric technologies?

221 **Federation and Assertions**

- 222 • What additional privacy considerations (e.g., revocation of consent, limitations of
223 use) may be required to account for the use of identity and provisioning APIs that
224 had not previously been discussed in the guidelines?
- 225 • Is the updated text and introduction of “bound authenticators” sufficiently clear
226 to allow for practical implementations of federation assurance level (FAL) 3
227 transactions? What complications or challenges are anticipated based on the
228 updated guidance?

229 **General**

- 230 • Is there an element of this guidance that you think is missing or could be expanded?
- 231 • Is any language in the guidance confusing or hard to understand? Should we add
232 definitions or additional context to any language?
- 233 • Does the guidance sufficiently address privacy?
- 234 • Does the guidance sufficiently address equity?
 - 235 – What equity assessment methods, impact evaluation models, or metrics
236 could we reference to better support organizations in preventing or detecting
237 disparate impacts that could arise as a result of identity verification
238 technologies or processes?
- 239 • What specific implementation guidance, reference architectures, metrics, or other
240 supporting resources may enable more rapid adoption and implementation of this
241 and future iterations of the Digital Identity Guidelines?
- 242 • What applied research and measurement efforts would provide the greatest impact
243 on the identity market and advancement of these guidelines?

244 Reviewers are encouraged to comment and suggest changes to the text of all four draft
245 volumes of of the NIST SP 800-63-4 suite. NIST requests that all comments be submitted
246 by 11:59pm Eastern Time on March 24, 2023. Please submit your comments to [dig-](mailto:dig-comments@nist.gov)
247 comments@nist.gov. NIST will review all comments and make them available at the
248 [NIST Identity and Access Management website](#). Commenters are encouraged to use the
249 comment template provided on the [NIST Computer Security Resource Center website](#).

250 **Call for Patent Claims**

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

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

- 260 a) assurance in the form of a general disclaimer to the effect that such party does not
261 hold and does not currently intend holding any essential patent claim(s); or
- 262 b) assurance that a license to such essential patent claim(s) will be made available
263 to applicants desiring to utilize the license for the purpose of complying with the
264 guidance or requirements in this ITL draft publication either:
 - 265 i. under reasonable terms and conditions that are demonstrably free of any unfair
266 discrimination; or
 - 267 ii. without compensation and under reasonable terms and conditions that are
268 demonstrably free of any unfair discrimination.

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

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

277 Such statements should be addressed to: <mailto:dig-comments@nist.gov>.

278	Table of Contents	
279	1. Purpose	2
280	2. Introduction	3
281	2.1. Scope & Applicability	4
282	2.2. How to Use this Suite of SPs	5
283	2.3. Enterprise Risk Management Requirements and Considerations	6
284	2.3.1. Security	7
285	2.3.2. Privacy	7
286	2.3.3. Equity	8
287	2.3.4. Usability	9
288	3. Definitions and Abbreviations	10
289	4. Digital Identity Model	11
290	4.1. Overview	11
291	4.2. Enrollment and Identity Proofing	14
292	4.3. Authentication and Lifecycle Management	17
293	4.3.1. Authenticators	17
294	4.3.2. Subscriber Accounts	19
295	4.3.3. Authentication Process	19
296	4.4. Federation and Assertions	20
297	4.4.1. Federation Benefits	21
298	4.4.2. Federation Protocols and Assertions	22
299	4.4.3. Relying Parties	22
300	5. Digital Identity Risk Management	23
301	5.1. Conduct Initial Impact Assessment	24
302	5.1.1. Identify Impacted Entities	24
303	5.1.2. Identify Impact Categories and Potential Harms	25
304	5.1.3. Identify Potential Impact Levels	26
305	5.1.4. Impact Analysis	29
306	5.2. Select Initial Assurance Levels	30
307	5.2.1. Assurance Levels	31

308	5.2.2. xAL Descriptions	31
309	5.2.3. Initial Assurance Level Selection	32
310	5.3. Tailor and Document Assurance Levels	36
311	5.3.1. Assess Privacy, Equity, Usability and Threats	37
312	5.3.2. Identify Compensating Controls	37
313	5.3.3. Identify Supplemental Controls	38
314	5.3.4. Document Results - The Digital Identity Acceptance Statement . .	38
315	5.4. Continuously Evaluate and Improve	39
316	5.5. Cyber, Fraud, and Identity Program Integrity	39
317	References	40
318	General References	40
319	Standards	41
320	NIST Special Publications	41
321	Federal Information Processing Standards	42
322	Appendix A. Definitions and Abbreviations	43
323	A.1. Definitions	43
324	A.2. Abbreviations	62
325	Appendix B. Change Log	67
326	B.1. SP 800-63-1	67
327	B.2. SP 800-63-2	67
328	B.3. SP 800-63-3	67
329	B.4. SP 800-63-4	68

330 **List of Tables**

331	1. Impact Categories	30
-----	--------------------------------	----

332 **List of Figures**

333	1. Non-Federated Digital Identity Model Example	12
334	2. Federated Digital Identity Model Example	13
335	3. Sample Identity Proofing and Enrollment Digital Identity Model	16
336	4. Sample Authentication Process	19

337 **Acknowledgments**

338 The authors would like to thank their fellow collaborators on the current revision of this
339 special publication, Christine Abruzzi, James L. Fenton, and Justin P. Richer, as well as
340 Kerriane Buchanan for her contributions and review. The authors would like to also
341 acknowledge the past contributions of Donna F. Dodson, Elaine M. Newton, Ray A.
342 Perlner, W. Timothy Polk, Emad A. Nabbus, Paul A. Grassi, Michael E. Garcia, Kaitlin
343 Boeckl, Joni Brennan, Ellen Nadeau, Ben Piccareta, and Danna Gabel O'Rourke.

344 **1. Purpose**

345 *This section is informative.*

346 This publication and its companion volumes, [SP800-63A], [SP800-63B], and
347 [SP800-63C], provide technical guidelines to organizations for the implementation of
348 digital identity services.

2. Introduction

This section is informative.

As the line between the virtual world and physical world blurs, and as digital and internet-enabled technologies continue to proliferate and connect, it is imperative that developers and consumers alike understand this changing hybrid ecosystem - including its associated opportunities and risks. Engagement across this ecosystem is often determined by an individual's ability and willingness to establish a digital identity - the unique representation of a person engaged in an online transaction.

A digital identity is always unique in the context of a digital service but does not always uniquely identify a person in all contexts. Further, while a digital identity may relay unique and specific meaning within the context of a digital service, the real-life identity of the individual behind the digital identity may not be known. For the purpose of this publication, a "person" refers to natural persons only (i.e., not all legal persons.)

Establishing a digital identity is intended to demonstrate trust between the holder of the digital identity and the person, organization, or system on the other side of the digital transaction. However, this process can present challenges. As in relationships and transactions in the physical world, there are multiple opportunities for mistakes, miscommunication, impersonation, and other attacks that fraudulently claim another person's digital identity. Additionally, given the broad range of individual needs, constraints, capacities, and preferences, digital services must be designed with equity and flexibility in mind to ensure broad and enduring participation.

Risks associated with digital identity stretch beyond the potential impacts to enterprises and should be incorporated into enterprise decision-making. This publication endeavors to more robustly and explicitly account for risks to individuals, communities, and other organizations. Specifically, while using this guidance, organizations should consider how decisions related to digital identity that prioritize organizational cybersecurity objectives might affect or need to accommodate other objectives, such as those related to privacy, equity, usability, and other indicators of mission and business performance that center the experiences of the individuals interacting with programs and services. By taking a human-centered and continuously informed approach to mission delivery, organizations have an opportunity to incrementally build trust with the variety of populations they serve, improve customer satisfaction, identify issues more quickly, and provide individuals with effective and culturally appropriate redress options.

These guidelines lay out a model for federal programs and other organizations to assess and manage risks associated with digital identity systems, including the processes, policies, data, people, and technologies that support digital identity management. The model is supported by a series of processes: identity proofing, authentication, and federation. The identity proofing process establishes that a subject is a specific physical person. The digital authentication process determines the validity of one or

388 more authenticators used to claim a digital identity and establishes confidence that a
389 subject attempting to access a digital service: (1) is in control of the technologies being
390 used for authentication, and (2) is the same subject that previously accessed the service.
391 Finally, the federation process allows for identity information to be shared in support of
392 authentication across systems.

393 The composition, model, and availability of identity services has significantly
394 changed since the first version of SP 800-63 was released, as have the considerations
395 and challenges of deploying secure, private, and equitable services to diverse user
396 communities. This revision addresses these challenges while facilitating the new models
397 and architectures for identity services that have developed by clarifying requirements
398 based on the function an entity may serve under the overall digital identity model.

399 Additionally, this publication provides instruction for credential service providers (CSPs),
400 verifiers, and relying parties (RPs) and it describes the risk management processes
401 that organizations should follow for implementing digital identity services and that
402 supplement the *NIST Risk Management Framework [NISTRMF]* and its component
403 special publications. The publication expands upon the NIST RMF by outlining how
404 equity and usability considerations should be incorporated into digital identity risk
405 management processes and it highlights the importance of considering impacts, not only
406 on the enterprise operations and assets, but also on individuals, other organizations, and,
407 more broadly, society. Further, while digital authentication supports privacy protection
408 by mitigating risks of unauthorized access to individuals' information, given that identity
409 proofing, authentication, authorization, and federation often involve the processing of
410 individuals' information, these functions can also create privacy risks. These guidelines,
411 therefore, include privacy requirements and considerations to help mitigate potential
412 associated privacy risks.

413 Finally, while this publication provides organizations with technical requirements and
414 recommendations for establishing, maintaining, and authenticating the digital identity
415 of subjects in order to access digital systems over a network, additional support options
416 outside the purview of information technology teams may need to be provided to address
417 barriers and adverse impacts, foster equity, and successfully deliver on mission objectives.

418 **2.1. Scope & Applicability**

419 Not all digital services require identity proofing or authentication; however, this guidance
420 applies to all online transactions for which some level of digital identity is required,
421 regardless of the constituency (e.g., citizens, business partners, and government entities).

422 These guidelines primarily focus on organizational services that interact with external
423 users, such as citizens accessing public benefits or private sector partners accessing
424 collaboration spaces. However, it also applies to federal systems accessed by employees
425 and contractors. The *Personal Identity Verification (PIV) of Federal Employees and*
426 *Contractors* standard [FIPS201] and its corresponding set of special publications and

427 organization-specific instructions, extend these guidelines for the federal enterprise,
428 providing additional technical controls and processes for issuing and managing Personal
429 Identity Verification (PIV) cards, binding additional authenticators as derived PIV
430 credentials, and using federation architectures and protocols with PIV systems.

431 Transactions not covered by this guidance include those associated with national security
432 systems as defined in 44 U.S.C. § 3542(b)(2). Private sector organizations and state, local,
433 and tribal governments whose digital processes require varying levels of digital identity
434 assurance may consider the use of these standards where appropriate.

435 Additionally, these technical guidelines do not address the identity of subjects for physical
436 access (e.g., to buildings), though some identities used for online transactions may also be
437 used for physical access. Additionally, this revision of these guidelines does not explicitly
438 address device identity, often referred to as machine-to-machine (such as router-to-router)
439 authentication or interconnected devices, commonly referred to as the internet of things
440 (IoT), although these guidelines are written to refer to generic subjects wherever possible
441 to leave open the possibility for applicability to devices. Furthermore, these guidelines
442 do not address authorization of access to Application Programming Interfaces (APIs) on
443 behalf of subjects.

444 **2.2. How to Use this Suite of SPs**

445 These guidelines support the mitigation of the negative impacts induced by a digital
446 identity error by separating the individual elements of digital identity into discrete,
447 component parts. For non-federated systems, agencies will select two components,
448 referred to as *Identity Assurance Level (IAL)* and *Authentication Assurance Level (AAL)*.
449 For federated systems, a third component, *Federation Assurance Level (FAL)*, is included.
450 [Sec. 5, Digital Identity Risk Management](#) provides details on the risk assessment process
451 and how the results of the risk assessment, with additional context, inform organizational
452 selection of IAL, AAL, and FAL combinations based on risk and mission.

453 By conducting appropriate risk management for business, security, and privacy, side-by-
454 side with mission needs, organizations will select IAL, AAL, and FAL as distinct options.
455 Specifically, organizations are required to individually select levels corresponding to each
456 function being performed. While many systems could have the same numerical level for
457 each IAL, AAL, and FAL, this is not a requirement and organizations should not assume
458 they will be the same in any given system or application.

459 The components of identity assurance detailed in these guidelines are as follows:

- 460 • **IAL** refers to the identity proofing process.
- 461 • **AAL** refers to the authentication process.
- 462 • **FAL** refers to the federation process, when the RP is connected through a federated
463 protocol.

464 Note: When described generically or bundled, these guidelines will refer to
465 IAL, AAL, and FAL as *xAL*.

466 SP 800-63 is organized as the following suite of volumes:

467 *SP 800-63 Digital Identity Guidelines*: Provides the risk assessment methodology and an
468 overview of general identity frameworks, using authenticators, credentials, and assertions
469 together in a digital system, and a risk-based process of selecting assurance levels. *SP*
470 *800-63 contains both normative and informative material*.

471 [\[SP800-63A\]](#): Provides requirements for enrollment and identity proofing of applicants,
472 either remotely or in person, that wish to gain access to resources at each of the three
473 identity assurance levels (IALs). It details the responsibilities of Credential Service
474 Providers (CSPs) with respect to establishing and maintaining subscriber accounts and
475 binding authenticators (either CSP-issued or subscriber-provided) to the subscriber
476 account. *SP 800-63A contains both normative and informative material*.

477 [\[SP800-63B\]](#): Provides recommendations on types of authentication processes, including
478 choices of authenticators, that may be used at each of the three authentication assurance
479 levels (AALs). It also provides recommendations on the lifecycle of authenticators,
480 including invalidation in the event of loss or theft. *SP 800-63B contains both normative*
481 *and informative material*.

482 [\[SP800-63C\]](#): Provides requirements on the use of federated identity architectures
483 and assertions to convey the results of authentication processes and relevant identity
484 information to an agency application. Further, this volume offers privacy-enhancing
485 techniques to share information about a valid, authenticated subject, and describes
486 methods that allow for strong multi-factor authentication (MFA) while the subject
487 remains pseudonymous to the digital service. *SP 800-63C contains both normative and*
488 *informative material*.

489 **2.3. Enterprise Risk Management Requirements and Considerations**

490 Effective enterprise risk management is multidisciplinary by default and involves the
491 consideration of a diverse set of factors and equities. In a digital identity risk management
492 context, these factors include, but are not limited to, information security, privacy, equity,
493 and usability. It is important for risk management efforts to weigh these factors as
494 they relate not only to enterprise assets and operations but also to individuals, other
495 organizations, and society more broadly.

496 During the process of analyzing factors relevant to digital identity, organizations may
497 determine that measures outside of those specified in this publication are appropriate in
498 certain contexts, for instance where privacy or other legal requirements exist or where the
499 output of a risk assessment leads the organization to determine that additional measures or
500 other process safeguards are appropriate. Organizations, including federal agencies, may

501 employ compensating or supplemental controls not specified in this publication. They
502 may also consider partitioning the functionality of a digital service to allow less sensitive
503 functions to be available at a lower level of assurance.

504 The considerations detailed below support enterprise risk management efforts and
505 encourage informed, inclusive, and human-centric service delivery. While this list of
506 considerations is not exhaustive, it highlights a set of cross-cutting factors likely to impact
507 decision-making associated with digital identity management.

508 **2.3.1. Security**

509 It is increasingly important for enterprise organizations to assess and manage digital
510 identity security risks, such as unauthorized access, availability issues, impersonation, and
511 other types of fraudulent claims, as well as institute strong identity governance practices.
512 As organizations consult this guidance, they should consider potential impacts to the
513 confidentiality, integrity, and availability of information and information systems that they
514 manage and that their service providers and business partners manage on behalf of the
515 individuals and communities that they serve.

516 Federal agencies implementing these guidelines need to adhere to their statutory
517 responsibilities, including those under the *Federal Information Security Modernization*
518 *Act (FISMA) of 2014* [FISMA] and related NIST standards and guidelines. NIST
519 recommends that non-federal organizations implementing these guidelines follow
520 equivalent standards to ensure the secure operation of their digital systems.

521 FISMA requires federal agencies to implement appropriate controls to protect federal
522 information and information systems from unauthorized access, use, disclosure,
523 disruption, or modification. The NIST RMF [NISTRMF] provides a process that
524 integrates security, privacy, and cyber supply chain risk management activities into the
525 system development life cycle. It is expected that federal agencies and organizations
526 that provide services under these guidelines have already implemented the controls and
527 processes required under FISMA and associated NIST risk management processes and
528 publications.

529 The controls and requirements encompassed by the identity, authentication, and
530 federation assurance levels under these guidelines augment, but do not replace or alter,
531 the information and information system controls as determined under FISMA and the
532 RMF.

533 **2.3.2. Privacy**

534 When designing, engineering, and managing digital identity systems, it is imperative to
535 consider the potential of that system to create privacy-related problems for individuals
536 when processing PII — a problematic data action — and the potential impact of the
537 problematic data action should it occur. Additionally, by focusing on the privacy

538 engineering objectives of predictability, manageability, and disassociability, organizations
539 can determine the types of capabilities a given system may need to be able to demonstrate
540 how organizational privacy policies and system privacy requirements have been
541 implemented.

542 The *Privacy Act of 1974, 2010 Edition*, [PrivacyAct] established a set of fair information
543 practices for the collection, maintenance, use, and disclosure of information about
544 individuals that is maintained by federal agencies in systems of records.

545 When designing and implementing digital identity management processes and systems,
546 privacy risk assessments are required for PII processing under these guidelines. Such
547 privacy risk assessments can be used to support Privacy Impact Assessments under *OMB*
548 *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
549 [M-03-22] as well as to select controls from NIST Special Publication 800-53, *Security*
550 *and Privacy Controls for Information Systems and Organizations* [SP800-53]. Further,
551 each volume of 800-63 (63A, 63B, and 63C) contains a specific section providing
552 detailed privacy requirements and considerations for the implementation of the processes,
553 controls, and requirements presented in that volume.

554 2.3.3. Equity

555 As defined in Executive Order 13985, *Advancing Racial Equity and Support for*
556 *Underserved Communities Through the Federal Government* [EO13985], equity refers
557 to the consistent and systematic fair, just, and impartial treatment of all individuals,
558 including individuals who belong to underserved communities that have been denied
559 such treatment, such as Black, Latino, and Indigenous and Native American persons,
560 Asian Americans and Pacific Islanders, and other persons of color; members of religious
561 minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons
562 with disabilities; persons who live in rural areas; and persons otherwise adversely affected
563 by persistent poverty or inequality.

564 A person's ability to engage in an online transaction, such as accessing a critical service
565 like healthcare, is often dependent on their ability to successfully and safely present a
566 digital identity. Given the broad disparities that exist in the U.S. society and globally,
567 many people are either unable to successfully present a digital identity, or they face a
568 higher degree of burden in navigating online services than their more privileged peers,
569 leaving them locked out of critical services or broader participation in the online world.
570 In a public service context, this poses a direct risk to successful mission delivery. In a
571 broader societal context, challenges related to digital access can exacerbate existing
572 inequities and continue systemic cycles of exclusion for historically marginalized and
573 underserved groups.

574 Readers of this guidance are encouraged to consider existing inequities faced by the
575 populations they serve to identify opportunities to design or operate digital identity
576 systems and processes in ways that best support their needs. Readers are also encouraged

577 to consider any potential or actual impact to the experiences and outcomes of these
578 populations, including disparities between populations, caused by the design or operation
579 of digital identity systems.

580 For federal agencies implementing these guidelines, EO 13985 directs federal agencies
581 to identify underserved communities for the programs and services that they provide and
582 to determine and address any systemic barriers to underserved communities to provide
583 equitable access to those programs and services. In alignment with the direction set
584 by EO 13985, federal agencies should determine potential barriers communities and
585 individuals may face to enrollment in and access to online benefits and services. They
586 should also identify whether programmatic changes may be necessary to advance equity.

587 **2.3.4. Usability**

588 Usability refers to the extent to which a system, product, or service can be used by
589 specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in
590 a specified context of use.

591 Similar to equity, usability requires an understanding of the people interacting with a
592 digital identity system or process, as well as their unique goals and context of use. To
593 provide an effective, efficient, and satisfactory experience, readers of this guidance should
594 take a holistic approach to considering the interactions that each user will engage in
595 throughout the process of enrolling in and authenticating to a service. Throughout the
596 design and development lifecycle of a digital identity system or process, it is important to
597 conduct usability evaluation with representative users performing realistic scenarios and
598 tasks in appropriate context of use.

599 Digital identity management processes should be designed and implemented so it is easy
600 for users to do the right thing, hard to do the wrong thing, and easy to recover when the
601 wrong thing happens.

602 **3. Definitions and Abbreviations**

603 See [Appendix A](#) for a complete set of definitions and abbreviations.

4. Digital Identity Model

This section is informative.

4.1. Overview

The SP 800-63 guidelines use digital identity models that reflect technologies and architectures currently available in the market. These models have a variety of entities and functions and vary in complexity. Simple models group functions, such as creating subscriber accounts and providing attributes, under a single entity. More complex models separate these functions among a larger number of entities. The entities and their associated functions found in digital identity models include:

Subject (represented by one of three roles):

- Applicant — the subject to be identity proofed
- Subscriber — the subject that has successfully completed the identity proofing process or has successfully completed authentication
- Claimant — the subject to be authenticated

Credential Service Provider (CSP): A trusted entity whose functions include identity proofing applicants to the identity service and the registration of authenticators to subscriber accounts. A *subscriber account* is the CSP's established record of the subscriber, the subscriber's attributes, and associated authenticators. A CSP may be an independent third party.

Relying Party (RP): An entity that relies upon the information in the subscriber account, or an identity provider (IdP) assertion when using federation, typically to process a transaction or grant access to information or a system.

Verifier: An entity whose function is to verify the claimant's identity by verifying the claimant's possession and control of one or more authenticators using an authentication protocol. To do this, the verifier needs to confirm the binding of the authenticators with the subscriber account and check that the subscriber account is active.

Identity Provider (IdP): An entity in a federated model that performs both the CSP and Verifier functions. The IdP is responsible for authenticating the subscriber and issuing assertions to communicate with one or more RPs.

The entities and interactions that comprise the non-federated digital identity model are illustrated in [Figure 1](#). The federated digital identity model is illustrated in [Figure 2](#).

[Figure 1](#) shows an example of a common sequence of interactions in the non-federated model. Other sequences could also achieve the same functional requirements. The usual sequence of interactions for identity proofing and enrollment activities is as follows:

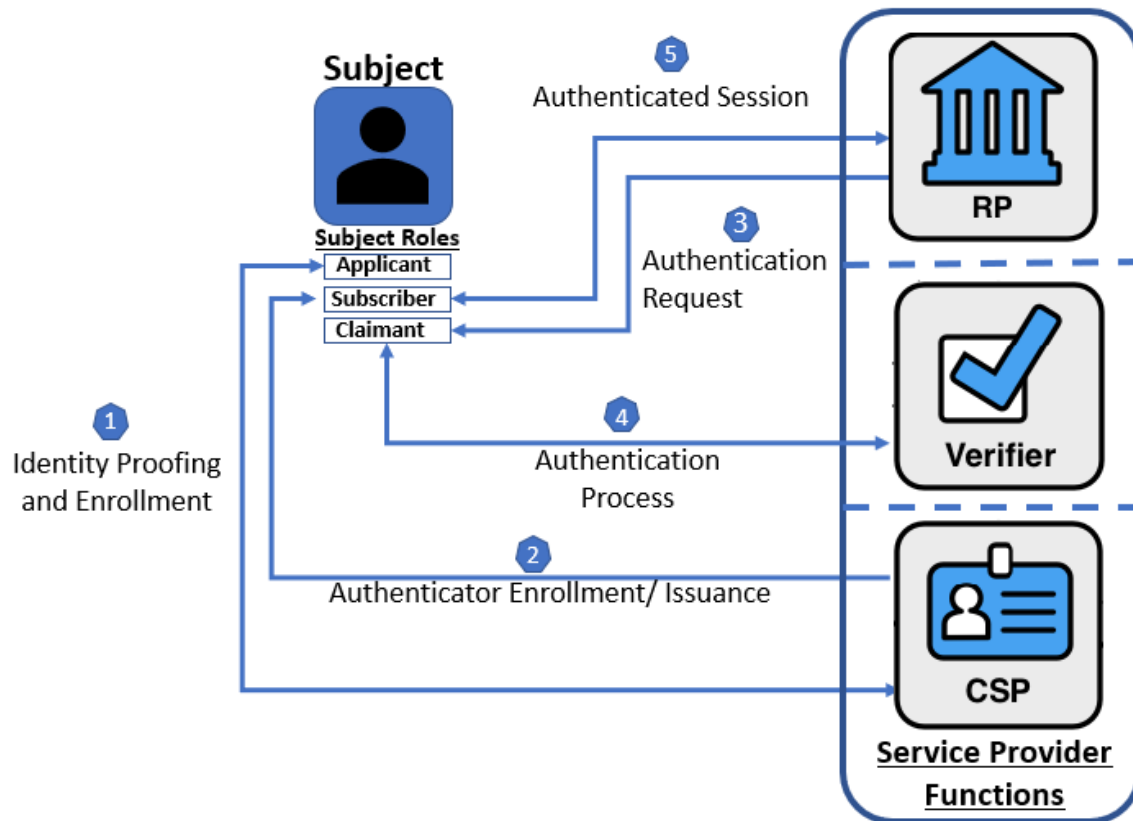


Figure 1. Non-Federated Digital Identity Model Example

- 638 • Step 1: An applicant applies to a CSP through an enrollment process. The CSP
639 identity proofs that applicant.
- 640 • Step 2: Upon successful proofing, the applicant is enrolled in the identity service as
641 a subscriber.
 - 642 – A subscriber account and corresponding authenticators are established
643 between the CSP and the subscriber. The CSP maintains the subscriber
644 account, its status, and the enrollment data. The subscriber maintains their
645 authenticators.

646 The usual sequence of interactions involved in using one or more authenticators to
647 perform digital authentication in the non-federated model is as follows:

- 648 • Step 3: The RP requests authentication from the claimant.
- 649 • Step 4: The claimant proves possession and control of the authenticators to the
650 verifier through an authentication process.

- 651 – The verifier interacts with the CSP to verify the binding of the claimant’s
652 identity to their authenticators in the subscriber account and to optionally
653 obtain additional subscriber attributes.
- 654 – The CSP or verifier functions of the service provider provide information
655 about the subscriber. The RP requests the attributes it requires from the CSP.
656 The RP, optionally, uses this information to make authorization decisions.
- 657 • Step 5: An authenticated session is established between the subscriber and the RP.

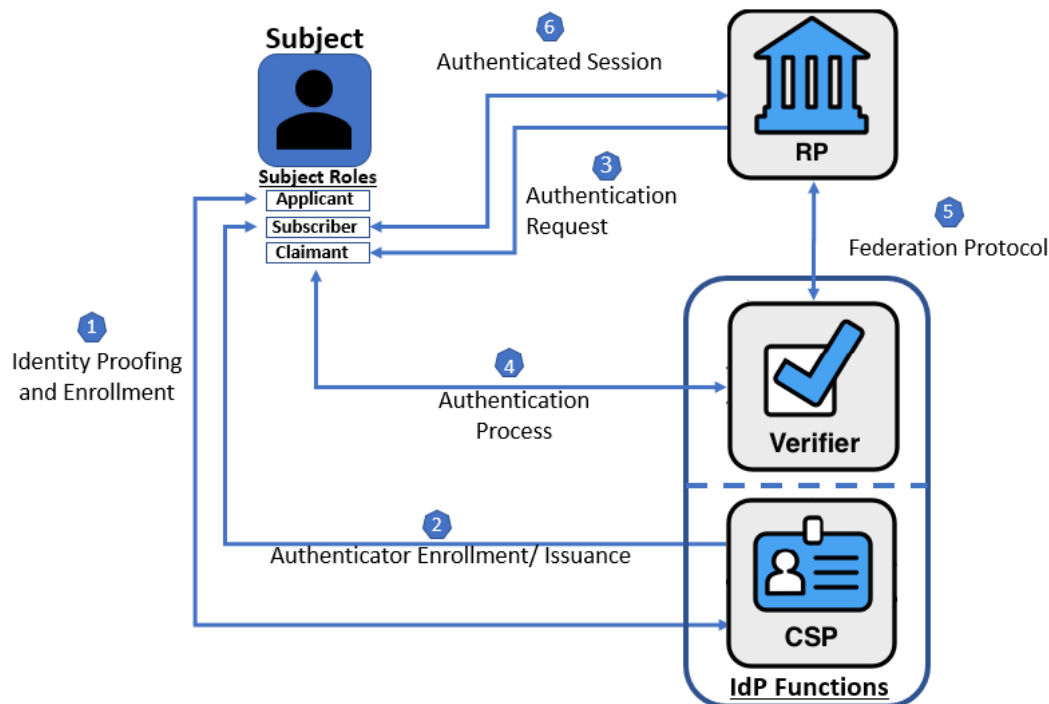


Figure 2. Federated Digital Identity Model Example

658 Figure 2 shows an example of those same common interactions in a federated model.

- 659 • Step 1: An applicant applies to an IdP through an enrollment process. Using its
660 CSP function, the IdP identity proofs the applicant.
- 661 • Step 2: Upon successful proofing, the applicant is enrolled in the identity service as
662 a subscriber.
- 663 – A subscriber account and corresponding authenticators are established
664 between the IdP and the subscriber. The IdP maintains the subscriber account,
665 its status, and the enrollment data collected for the lifetime of the subscriber
666 account (at a minimum). The subscriber maintains their authenticators.

667 The usual sequence of interactions involved in using one or more authenticators in the
668 federated model to perform digital authentication is as follows:

- 669 • Step 3: The RP requests authentication from the claimant. The IdP provides
670 an assertion and optionally additional attributes to the RP through a federation
671 protocol.
- 672 • Step 4: The claimant proves possession and control of the authenticators to the
673 verifier function of the IdP through an authentication process.
 - 674 – Within the IdP, the verifier and CSP functions interact to verify the binding
675 of the claimant’s authenticators with those bound to the claimed subscriber
676 account and optionally to obtain additional subscriber attributes.
- 677 • Step 5: All communication, including assertions, between the RP and the IdP
678 happens through federation protocols.
- 679 • Step 6: The IdP provides the RP with the authentication status of the subscriber
680 and relevant attributes and an authenticated session is established between the
681 subscriber and the RP.

682 For both models, the verifier does not always need to communicate in real time with
683 the CSP to complete the authentication activity (e.g., some uses of digital certificates).
684 Therefore, the line between the verifier and the CSP represents a logical link between
685 the two entities. In some implementations, the verifier, RP, and CSP functions may
686 be distributed and separated. However, if these functions reside on the same platform,
687 the interactions between the functions are signals between applications or application
688 modules running on the same system rather than using network protocols.

689 In all cases, the RP should request the attributes it requires from a CSP or IdP before
690 authenticating the claimant.

691 The following sections provide more detailed digital identity models for identity proofing,
692 authentication, and federation.

693 **4.2. Enrollment and Identity Proofing**

694 The previous section introduced the entities and interactions in the conceptual digital
695 identity model. This section provides additional details regarding the participants’
696 relationships and responsibilities with respect to identity proofing and enrollment
697 processes.

698 [SP800-63A], *Enrollment and Identity Proofing* provides general information and
699 normative requirements for the identity proofing and enrollment processes as well as
700 requirements specific to identity assurance levels (IALs). In addition to a “no identity
701 proofing” level, IAL0, this document defines three IALs that indicate the relative strength
702 of an identity proofing process.

703 An individual, referred to as an *applicant* at this stage, opts to enroll with a CSP. If the
704 applicant is successfully proofed, the individual is then enrolled in the identity service as
705 a *subscriber* of that CSP.

706 The CSP then establishes a subscriber account to uniquely identify each subscriber and
707 record any authenticators registered (bound) to that subscriber account. The CSP may:

- 708 • issue one or more authenticators to the subscriber at the time of enrollment,
- 709 • bind authenticators provided by the subscriber, and/or
- 710 • bind authenticators to the subscriber account at a later time as needed.

711 CSPs generally maintain subscriber accounts according to a documented lifecycle, which
712 defines specific events, activities, and changes that affect the status of a subscriber
713 account. CSPs generally limit the lifetime of a subscriber account and any associated
714 authenticators in order to ensure some level of accuracy and currency of attributes
715 associated with a subscriber. When there is a status change or when the authenticators
716 near expiration and any renewal requirements are met, they may be renewed and/or re-
717 issued. Alternately, the authenticators may be invalidated and destroyed according to the
718 CSPs written policy and procedures.

719 Subscribers have a duty to maintain control of their authenticators and comply with CSP
720 policies in order to remain in good standing with the CSP.

721 In order to request issuance of a new authenticator, typically the subscriber authenticates
722 to the CSP using their existing, unexpired authenticators. If the subscriber fails to request
723 authenticator re-issuance prior to their expiration or revocation, they may be required to
724 repeat the identity proofing (either complete or abbreviated) and enrollment processes in
725 order to obtain a new authenticator.

726 [Figure 3](#) shows a sample of interactions for identity proofing and enrollment.

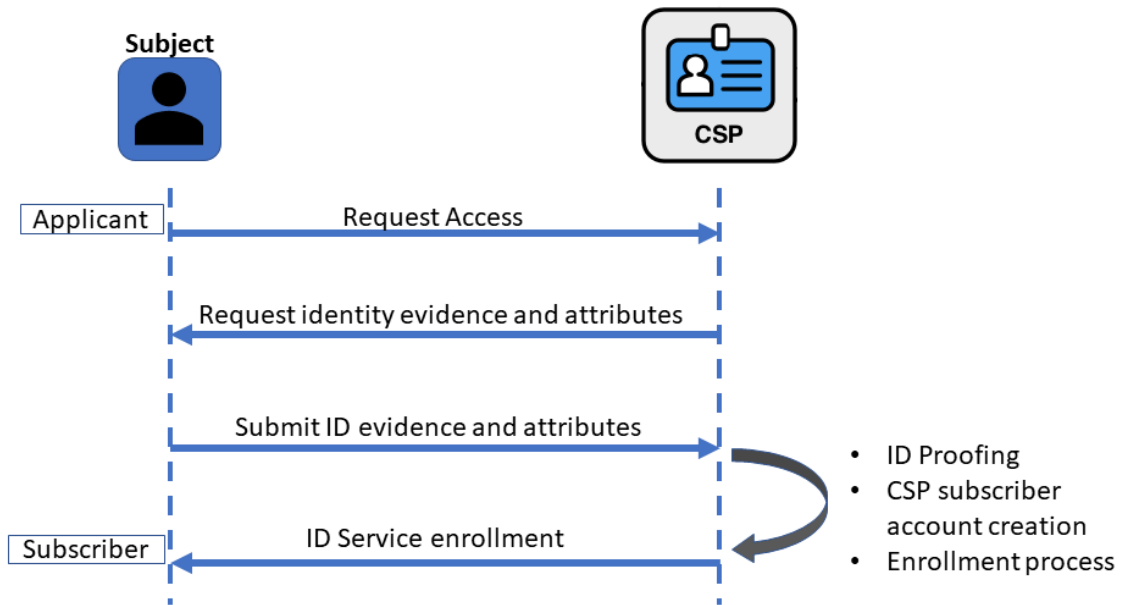


Figure 3. Sample Identity Proofing and Enrollment Digital Identity Model

727 **4.3. Authentication and Lifecycle Management**

728 Normative requirements can be found in [SP800-63B], *Authentication and Lifecycle*
729 *Management*.

730 **4.3.1. Authenticators**

731 The classic paradigm for authentication systems identifies three factors as the
732 cornerstones of authentication:

- 733 • Something you know (e.g., a password)
- 734 • Something you have (e.g., an ID badge or a cryptographic key)
- 735 • Something you are (e.g., a fingerprint or other biometric characteristic data)

736 Single-factor authentication requires only one of the above factors, most often
737 “something you know”. Multiple instances of the same factor still constitute single-factor
738 authentication. For example, a user generated PIN and a password do not constitute two
739 factors as they are both “something you know.” Multi-factor authentication (MFA) refers
740 to the use of more than one distinct factor. For the purposes of these guidelines, using two
741 factors is adequate to meet the highest security requirements. Other types of information,
742 such as location data or device identity, may also be used by a verifier to evaluate the risk
743 in a claimed identity but they are not considered authentication factors.

744 In digital authentication, the claimant possesses and controls one or more authenticators.
745 The authenticators will have been bound with the subscriber account. The authenticators
746 contain secrets the claimant can use to prove they are a legitimate subscriber. The
747 claimant authenticates to a system or application over a network by demonstrating they
748 have possession and control of the authenticator. Once authenticated, the claimant is
749 referred to as a subscriber.

750 The secrets contained in an authenticator are based on either key pairs (asymmetric
751 cryptographic keys) or shared secrets (including symmetric cryptographic keys and
752 memorized secrets). Asymmetric key pairs are comprised of a public key and a related
753 private key. The private key is stored on the authenticator and is only available for
754 use by the claimant who possesses and controls the authenticators. A verifier that has
755 the subscriber’s public key, for example through a public key certificate, can use an
756 authentication protocol to verify the claimant has possession and control of the associated
757 private key contained in the authenticators and, therefore, is a subscriber.

758 As mentioned above, shared secrets stored on an authenticator may be either symmetric
759 keys or memorized secrets (e.g., passwords and PINs). While both keys and memorized
760 secrets can be used in similar protocols, one important difference between the two is
761 how they relate to the claimant. Symmetric keys are generally chosen at random and
762 are complex and long enough to thwart network-based guessing attacks, and stored in
763 hardware or software that the subscriber controls. Memorized secrets typically have fewer

764 characters and less complexity than cryptographic keys to facilitate memorization and
765 ease of entry. The result is that memorized secrets have increased vulnerabilities that
766 require additional defenses to mitigate.

767 There is another type of memorized secret used as an activation factor for a multi-factor
768 authenticator. These are referred to as activation secrets. An activation secret is used to
769 decrypt a stored key used for authentication or is compared against a locally held stored
770 verifier to provide access to the authentication key. In either of these cases, the activation
771 secret remains within the authenticator and its associated user endpoint. An example of an
772 activation secret would be the PIN used to activate a PIV card.

773 As used in these guidelines, authenticators always contain or comprise a secret; however,
774 some authentication methods used for in-person interactions do not apply directly to
775 digital authentication. For example, a physical driver's license is something you have
776 and may be useful when authenticating to a human (e.g., a security guard) but it is not an
777 authenticator for online services.

778 Some commonly used authentication methods do not contain or comprise secrets, and are
779 therefore not acceptable for use under these guidelines. For example:

- 780 • Knowledge-based authentication, where the claimant is prompted to answer
781 questions that are presumably known only by the claimant, does not constitute
782 an acceptable secret for digital authentication.
- 783 • A biometric also does not constitute a secret and can not be used as a single-factor
784 authenticator.

785 A digital authentication system may incorporate multiple factors in one of two ways:

- 786 1. The system may be implemented so that multiple factors are presented to the
787 verifier, or
- 788 2. Some factors may be used to protect a secret that will be presented to the verifier.

789 For example, item 1 can be satisfied by pairing a memorized secret (something you
790 know) with an out-of-band device (something you have). Both authenticator outputs
791 are presented to the verifier to authenticate the claimant. For item 2, the authenticator
792 and authenticator secret could be a piece of hardware that contains a cryptographic key
793 (something you have) that is controlled by the claimant where access is protected with a
794 fingerprint (something you are). When used with the biometric factor, the cryptographic
795 key produces an output that is used to authenticate the claimant.

796 As noted above, biometrics do not constitute acceptable secrets for digital authentication
797 and, therefore, cannot be used for single-factor authentication. However, biometrics
798 authentication can be used as an authentication factor for multi-factor authentication when
799 used in combination with a possession-based authenticator. Biometric characteristics
800 are unique, personal attributes that can be used to verify the identity of a person who is

801 physically present at the point of verification. This includes, but is not limited to, facial
802 features, fingerprints, iris patterns, and voiceprints.

803 4.3.2. Subscriber Accounts

804 As described in the preceding sections, a subscriber account binds one or more
805 authenticators to the subscriber via an identifier as part of the registration process. A
806 subscriber account is created, stored, and maintained by the CSP. The subscriber account
807 records all identity attributes validated during the identity proofing process.

808 4.3.3. Authentication Process

809 The authentication process enables an RP to trust that a claimant is who they say they
810 are. Figure 4 shows a sample authentication process. Other approaches are described in
811 [SP800-63B], *Authentication and Lifecycle Management*. This sample authentication
812 process shows interactions between the RP, a claimant, and a verifier/CSP. The verifier is
813 a functional role and is frequently implemented in combination with the CSP, as shown in
814 Fig. 4, the RP, or both.

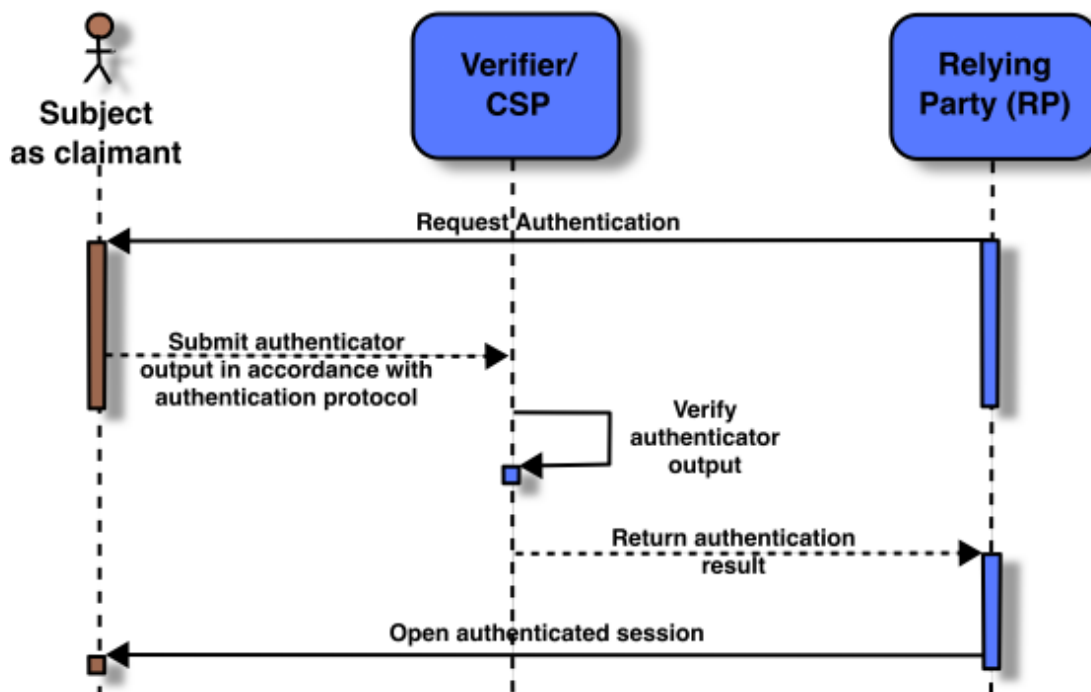


Figure 4. Sample Authentication Process

815 A successful authentication process demonstrates that the claimant has possession and
816 control of one or more valid authenticators that are bound to the subscriber's identity. In
817 general, this is done using an authentication protocol involving an interaction between
818 the verifier and the claimant. The exact nature of the interaction is extremely important

819 in determining the overall security of the system. Well-designed protocols can protect the
820 integrity and confidentiality of communication between the claimant and the verifier both
821 during and after the authentication, and can help limit the damage that can be done by an
822 attacker masquerading as a legitimate verifier.

823 Additionally, mechanisms located at the verifier can mitigate online guessing attacks
824 against lower entropy secrets — like passwords and PINs — by limiting the rate at which
825 an attacker can make authentication attempts, or otherwise delaying incorrect attempts.
826 Generally, this is done by keeping track of and limiting the number of unsuccessful
827 attempts, since the premise of an online guessing attack is that most attempts will fail.

828 **4.4. Federation and Assertions**

829 Normative requirements can be found in [SP800-63C], *Federation and Assertions*.

830 In general usage, the term *federation* can be applied to a number of different approaches
831 involving the sharing of information between different trust domains. These approaches
832 differ based on the kind of information that is being shared between the domains. Some
833 common examples include:

- 834 • sharing identifiers (e.g., using a driver’s license number or an email address),
- 835 • sharing authenticators (e.g., using a PKI authenticator for multiple applications),
- 836 • sharing identity assertions (e.g., a federation protocol like OpenID Connect or
837 SAML),
- 838 • sharing account attributes (e.g., a provisioning protocol like SCIM), and
- 839 • sharing authorization decisions (e.g., a policy protocol like XACML).

840 The SP 800-63 guidelines are agnostic to the identity proofing, authentication, and
841 federation architectures an organization selects and they allow organizations to deploy a
842 digital identity scheme according to their own requirements. However, there are scenarios
843 that an organization may encounter that make federation potentially more efficient
844 and effective than establishing identity services local to the organization or individual
845 applications. The following lists detail scenarios where the organization may consider
846 federation a viable option. These lists are provided for consideration and are not intended
847 to be comprehensive.

848 An organization should consider accepting federated identity assertions if any of the
849 following apply:

- 850 1. Potential users already have an authenticator at or above the required AAL.
- 851 2. Multiple types of authenticators are required to cover all possible user communities.
- 852 3. An organization does not have the necessary infrastructure to support management
853 of subscriber accounts (e.g., account recovery, authenticator issuance, help desk).

- 854 4. There is a desire to allow primary authenticators to be added and upgraded over
855 time without changing the RP's implementation.
- 856 5. There are different environments to be supported, as federation protocols are
857 network-based and allow for implementation on a wide variety of platforms and
858 languages.
- 859 6. Potential users come from multiple communities, each with its own existing identity
860 infrastructure.
- 861 7. The ability to centrally manage account lifecycles, including account revocation and
862 binding of new authenticators is important.

863 An organization should consider accepting federated identity attributes if any of the
864 following apply:

- 865 1. Pseudonymity is required, necessary, feasible, or important to stakeholders
866 accessing the service.
- 867 2. Access to the service requires a partial attribute list.
- 868 3. Access to the service requires at least one derived attribute value.
- 869 4. The organization is not the authoritative source or issuing source for required
870 attributes.
- 871 5. Attributes are only required temporarily during use (such as to make an access
872 decision), and the organization does not need to retain the data.

873 **4.4.1. Federation Benefits**

874 Federated architectures have many significant benefits, including, but not limited to:

- 875 • Enhanced user experience: For example, an individual can be identity proofed once
876 and reuse the subscriber account at multiple RPs.
- 877 • Cost reduction to both the user (reduction in authenticators) and the organization
878 (reduction in information technology infrastructure).
- 879 • Minimizing data in applications as organizations do not need to collect, store, or
880 dispose of personal information.
- 881 • Minimizing data exposed to applications, using pseudonymous identifiers and
882 derived attribute values instead of copying account values to each application.
- 883 • Mission enablement: Organizations can focus on their mission without worrying
884 about expending resources on identity management.

885 The following sections discuss the components of a federated identity architecture should
886 an organization elect this type of model.

887 **4.4.2. Federation Protocols and Assertions**

888 Federation protocols allow for the conveyance of assertions, authentication attributes,
889 and subscriber attributes across networked systems. In a federation scenario, as shown in
890 **Figure 2**, the CSP provides a service known as an identity provider, or IdP. The IdP acts as
891 a verifier for authenticators issued by the CSP. Using federation protocols, the IdP sends
892 a message, called an assertion, about this authentication event to the RP. Assertions are
893 verifiable statements from an IdP to an RP that represent an authentication event for a
894 subscriber. The RP receives and uses the assertion provided by the IdP, but the RP does
895 not verify authenticators directly.

896 Federation is generally used when the RP and the IdP are not a single entity or are not
897 under common administration, though this technology can be applied within a single
898 security domain for a variety of reasons. The RP uses the information in the assertion to
899 identify the subscriber and make authorization decisions about their access to resources
900 controlled by the RP.

901 Examples of assertions include:

- 902 • Security Assertion Markup Language (SAML) assertions are specified using a
903 mark-up language intended for describing security assertions. They can be used
904 by a verifier to make a statement to an RP about the identity of a claimant. SAML
905 assertions may optionally be digitally signed.
- 906 • OpenID Connect claims are specified using JavaScript Object Notation (JSON) for
907 describing security, and optionally, user claims. JSON user information claims may
908 optionally be digitally signed.
- 909 • Kerberos tickets allow a ticket-granting authority to issue session keys to two
910 authenticated parties using symmetric or asymmetric key establishment schemes.

911 **4.4.3. Relying Parties**

912 An RP relies on results of an authentication protocol to establish confidence in the
913 identity or attributes of a subscriber for the purpose of conducting an online transaction.
914 RPs may use a subscriber's federated identity (pseudonymous or non-pseudonymous),
915 IAL, AAL, FAL, and other factors to make authorization decisions.

916 When using federation, the verifier is not a function of the RP. A federated RP receives an
917 assertion from the IdP, which provides the verifier function, and the RP ensures that the
918 assertion came from an IdP that is trusted by the RP. The RP also processes any additional
919 information in the assertion, such as personal attributes or expiration times. The RP is
920 the final arbiter concerning whether a specific assertion presented by a verifier meets the
921 RP's established criteria for system access regardless of IAL, AAL, or FAL.

5. Digital Identity Risk Management

This section is normative.

This section provides details on the methodology for assessing digital identity risks for each xAL. This process augments the risk management processes for information and information system risk under NIST guidance for implementing Federal Information Security Modernization Act [FISMA] requirements.

There are 4 steps to the digital identity risk management process:

- 1. Conduct Initial Impact Assessment:** In this step, organizations evaluate their user population and assess the impact of a failure of each function in the identity system (i.e., proofing, authentication, and federation) for their protected application or service against a defined set of impact categories. The outcome of this step is a documented set of impact categories and associated impact levels.
- 2. Select Initial Assurance Levels:** In this step, the impact categories and impact levels are evaluated to determine the appropriate assurance levels to protect the application. The outcome of this step is an identified initial level for each applicable xAL.
- 3. Tailor and Document Assurance Level Determinations:** In this step, detailed privacy, equity, usability, and threat assessments are conducted to determine the potential impact of the initially selected assurance level on the specific user population and threat environment of the application. The initial assurance level is tailored, compensating or supplemental controls are identified, and all decisions are documented. The outcome is a Digital Identity Acceptance Statement (see [Sec. 5.3.4](#)) with a defined implementable assurance level.
- 4. Continuously Evaluate & Improve:** In this step, information is collected on performance of the identity system across a diverse set of factors based on organization needs and evolving threat vectors. This information is used to determine if the selected assurance level and controls are meeting mission, business, and security needs and to monitor for unintended harms that may have emerged. The outcomes of this step are performance metrics, documented and transparent processes for evaluation and redress, and ongoing improvements to the identity system as needed.

While presented as a “stepwise” approach, there can be many points in the process that require divergence from the sequential order, including the need for iterative cycles between initial task execution and revisiting tasks. For example, the introduction of new regulations or requirements while an assessment is ongoing may require organizations to revisit a step in the process. Additionally new functionality, changes in data usage, and changes to the threat environment may at any point require an organization to revisit steps in the digital identity risk management process.

960 Organizations **SHOULD** adapt and modify this overall approach to meet organizational
961 processes, governance, and integration with enterprise risk management practices. At a
962 minimum, organizations **SHALL** ensure that each step is executed and the normative
963 mandates and outcomes of each step are completed and documented regardless of
964 operational approach and enabling tools.

965 **5.1. Conduct Initial Impact Assessment**

966 The purpose of the initial impact analysis is to identify the potential adverse impacts of
967 failures in identity proofing, authentication, and federation specific to an RP application
968 or service, yielding an initial set of assurance levels. Assessing these areas separately
969 allows organizations maximum flexibility in developing or acquiring a digital identity
970 service that best enables them to successfully deliver on mission objectives.

971 The impact assessment includes:

- 972 • Identifying impacted entities,
- 973 • Identifying a set of impact categories for which harms will be assessed,
- 974 • Identifying potential harms for each of the impact categories,
- 975 • Identifying the levels of impact those potential harms would inflict should failures
976 occur, and
- 977 • Assessing the impact of each type of failure (proofing, authentication, and
978 federation) and the resulting impact level to all affected entities.

979 The output of this assessment is a defined impact level — High, Moderate, or Low — for
980 each possible type of failure. This serves as the primary input to the initial assurance level
981 selection.

982 **5.1.1. Identify Impacted Entities**

983 When assessing impacts, an organization needs to determine the entities that will be
984 impacted by the application or transaction under consideration. As mentioned earlier
985 in this guideline, it is imperative to consider the impact on different entities resulting
986 from a failure of the digital identity system. Of particular importance is ensuring that the
987 potential impacts to individuals are considered alongside those of the enterprise.

988 Accordingly, impact assessments **SHALL** include individuals using the system or
989 application in addition to the organization itself. Additionally, organizations **SHOULD**
990 identify other entities, such as mission partners, communities, and those identified in
991 [SP800-30], that need to be specifically included based on mission and business needs.
992 At a minimum, agencies **SHALL** document all entities to which impacts will be assessed
993 when conducting their impact analysis.

994 The outcome of this activity is a list of entities subject to the application or transaction
995 under consideration for whom impacts will be assessed.

5.1.2. Identify Impact Categories and Potential Harms

Initial assurance levels for digital transactions **SHALL** be determined by assessing the potential impact of, at a minimum, each of the following categories:

- Damage to mission delivery
- Damage to trust or reputation
- Loss of sensitive information
- Damage to or loss of economic stability
- Loss of life or damage to safety, health, or environmental stability
- Noncompliance with laws, regulations, and/or contractual obligations

Organizations **SHOULD** include additional impact categories as appropriate based on their mission. Each impact category **SHALL** be documented and consistently applied across different applications assessed by the organization.

Harms are any adverse effects that would be experienced by an entity. They provide a means to more effectively understand the impact categories and how they may apply to specific entities associated with that application. Agencies **SHOULD** consider specific harms for each of the defined impact categories to better inform their impact analysis. Identification of harms for each category **SHALL** be done for each of the entities identified during “entity identification” process.

Examples of harms associated with each category include, but are not limited to:

Damage to mission delivery:

- Harms to individuals may include the inability to access government services or benefits for which they are eligible.
- Harms to the organization may include an inability to perform current mission/business functions in a sufficiently timely manner, with sufficient confidence and/or correctness, within planned resource constraints, or an inability, or limited ability, to perform mission/business functions in the future.

Damage to trust or reputation:

- Harms to individuals may include impersonation or damage to image or reputation.
- Harms to the organization may include damage to trust relationships, image, or reputation including future, potential trust relationships.

Loss of sensitive information:

- Harms to individuals includes loss of PII or other sensitive information, which may result in secondary harms such as loss of economic stability, loss of life, physical or psychological injury, impersonation, identity theft, or persistent inconvenience.

- 1030 • Harms to the organization may include loss or degradation of intellectual property
1031 or other information assets such as classified materials or controlled unclassified
1032 information (CUI).

1033 Damage to or loss of economic stability:

- 1034 • Harms to individuals may include debts incurred or assets lost as a result of fraud or
1035 other harm, damage to or loss of credit, actual or potential employment, or sources
1036 of income, and/or other financial loss.
- 1037 • Harms to the organization may include costs incurred related to fraud or other
1038 criminal activity, loss of assets, devaluation, or loss of business.

1039 Loss of life or damage to safety, health, or environmental stability:

- 1040 • Harms to individuals may include death, damage to or loss of physical, mental, or
1041 emotional well-being, damage to the environment, or loss of accessible, affordable
1042 housing.
- 1043 • Harms to the organization may include damage to or loss of the organization's
1044 workforce or the impact of unsafe conditions rendering the organization unable to
1045 operate or operating at reduced capacity.

1046 Noncompliance with laws, regulations, and/or contractual obligations:

- 1047 • Harms to individuals may include damage to or loss of economic stability, safety,
1048 privacy, civil liberties, equity, and/or usability due to violations of local, state, and
1049 federal laws, regulations, and/or contractual obligations.
- 1050 • Harms to the organization may include financial costs, sanctions, liability, etc, due
1051 to noncompliance with applicable laws, regulations, contractual requirements, or
1052 other requirements in other binding agreements.

1053 The outcome of this activity will be a list of impact categories and harms which will be
1054 used to assess impacts to identified entities.

1055 **5.1.3. Identify Potential Impact Levels**

1056 Initial assurance levels for digital transactions are determined by assessing the potential
1057 impact a failure would have on each of the categories from [Sec. 5.1.2](#) using one of the
1058 following potential impact values:

- 1059 1. Low potential impact: could be expected to have a limited adverse effect
- 1060 2. Moderate potential impact: could be expected to have a serious adverse effect
- 1061 3. High potential impact: could be expected to have a severe or catastrophic adverse
1062 effect

1063 Note: If a failure in the identity system causes no measurable consequences
1064 for a category, there is no impact.

1065 Each assurance level, IAL, AAL, and FAL (if accepting or asserting a federated identity)
1066 **SHALL** be evaluated separately. Ideally, any evaluation will include different viewpoints
1067 such as harm to individuals, the organization, other organizations, and the nation as
1068 applicable to successful delivery of the organization's mission. Examples of potential
1069 impacts in each of the categories include:

1070 **Damage to mission delivery:**

- 1071 • **Low:** at worst, slight outcome disparities exist between individuals that participate
1072 in federally funded programs and those that are eligible but unable to participate, or
1073 a limited adverse effect on organizational operations or assets, or public interests.
1074 Examples of limited adverse effects are: mission capability degradation to the
1075 extent and duration that the organization is able to perform its primary functions
1076 with noticeably reduced effectiveness, or minor damage to organizational assets or
1077 public interests.
- 1078 • **Moderate:** at worst, outcome disparities are evident between individuals that
1079 participate in federally funded programs and those that are eligible but unable
1080 to participate, or a serious adverse effect on organizational operations or assets,
1081 or public interests. Examples of serious adverse effects are: significant mission
1082 capability degradation to the extent and duration that the organization is able
1083 to perform its primary functions with significantly reduced effectiveness; or
1084 significant damage to organizational assets or public interests.
- 1085 • **High:** outcome disparities endure across communities, indicating a systemic
1086 pattern of exclusion, avoidance, or other barriers to participation in federally
1087 funded programs, or a severe or catastrophic adverse effect on organizational
1088 operations or assets, or public interests. Examples of severe or catastrophic effects
1089 are: severe mission capability degradation or loss to the extent and duration that the
1090 organization is unable to perform one or more of its primary functions; or major
1091 damage to organizational assets or public interests.

1092 **Damage to trust and reputation:**

- 1093 • **Low:** at worst, limited, short-term inconvenience, distress, or embarrassment to any
1094 party.
- 1095 • **Moderate:** at worst, serious short-term or limited long-term inconvenience, distress,
1096 or damage to the standing or reputation of any party.
- 1097 • **High:** severe or serious long-term inconvenience, distress, or damage to the
1098 standing or reputation of any party. This is ordinarily reserved for situations with
1099 particularly severe effects or which potentially affect many individuals.

1100

- 1101 • **Low:** at worst, a limited release of personal, U.S. government sensitive, or
1102 commercially sensitive information to unauthorized parties resulting in a loss of
1103 confidentiality with a low impact as defined in [FIPS199].
- 1104 • **Moderate:** at worst, a release of personal, U.S. government sensitive, or
1105 commercially sensitive information to unauthorized parties resulting in loss of
1106 confidentiality with a moderate impact as defined in [FIPS199].
- 1107 • **High:** a release of personal, U.S. government sensitive, or commercially sensitive
1108 information to unauthorized parties resulting in loss of confidentiality with a high
1109 impact as defined in [FIPS199].

1110 **Damage to or loss of economic stability:**

- 1111 • **Low:** at worst, an insignificant or inconsequential financial loss to any party.
- 1112 • **Moderate:** at worst, a serious financial loss to any party.
- 1113 • **High:** severe or catastrophic financial loss to any party.

1114 **Loss of life or damage to safety, health, or environmental stability:**

- 1115 • **Low:** at worst, minor injury or acute health issue that resolves itself and does not
1116 require medical, including mental health, treatment; limited risk of environmental
1117 impact in locality where program operations take place.
- 1118 • **Moderate:** at worst, moderate risk of minor injury or limited risk of injury
1119 requiring medical, including mental health, treatment; or the compounding impact
1120 of multiple low impact events; moderate risk of environmental impact in locality
1121 where program operations take place.
- 1122 • **High:** a risk of serious injury, trauma, or death; or the compounding impact of
1123 multiple moderate impact events; high risk of environmental impact in locality
1124 where program operations take place.

1125 **Noncompliance with laws, regulations, and/or contractual obligations:**

- 1126 • **Low:** at worst, a risk of civil or criminal violations of a nature that would not
1127 ordinarily be subject to enforcement efforts, or at worst, an insignificant or
1128 inconsequential organization liability.
- 1129 • **Moderate:** at worst, a risk of civil or criminal violations that may be subject to
1130 enforcement efforts, or a serious organization liability.
- 1131 • **High:** a risk of civil or criminal violations that are of special importance to
1132 enforcement programs, or severe or catastrophic organization liability.

1133 **5.1.4. Impact Analysis**

1134 The impact analysis helps determine the extent to which risk must be mitigated by the
1135 identity proofing, authentication, and federation processes. These determinations drive
1136 the relevant choices of applicable technologies and mitigation strategies, rather than the
1137 desire for any given technology driving risk determinations.

1138 To determine the appropriate level of assurance of the user's asserted identity,
1139 organizations **SHALL** assess the potential risks and identify measures to minimize
1140 their impact. Organizations **SHALL** assess the risk of identity proofing, authentication,
1141 and federation failures separately to determine the required assurance level for each
1142 transaction. This process **SHALL** include consideration of potentially varying impacts
1143 of harms to different entities impacted by the digital identity system, as described in
1144 [Sec. 5.1.1](#). Business processes, policies, and technologies may help reduce risk. Entities
1145 **SHOULD** consider the impact of specific modes of failures related to identity proofing,
1146 authentication, and federation this includes, but may not be limited to:

1147 **Identity Proofing:**

- 1148 • The impact of providing a service to the wrong subject (e.g., an attacker
1149 successfully proves as someone else).
- 1150 • The impact of not providing service to an eligible subject due to barriers, including
1151 biases, faced by the subject throughout the process of identity proofing.
- 1152 • The impact of excessive information collection and retention to support identity
1153 proofing processes.

1154 **Authentication:**

- 1155 • The impact of authenticating the wrong subject (e.g., an attacker who compromises
1156 or steals an authenticator).
- 1157 • The impact of failing to authenticate the correct subject due to barriers, including
1158 biases, faced by the subject in presenting their authenticator.

1159 **Federation:**

- 1160 • The impact of the wrong subject successfully accessing an application, system, or
1161 data (e.g., compromising or replaying an assertion).
- 1162 • The impact of releasing subscriber attributes to the wrong application or system.

1163 Using a worksheet similar to [Table 1](#) can assist organizations with compiling the
1164 information gathered in order to complete the analysis. This kind of analysis would be
1165 done for each type of potential failure for identity proofing, authentication, and federation
1166 to determine the overall risks to entities interacting with the digital identity system.

Table 1. Impact Categories

Impact Categories	Harm to Individuals	Harm to the Organization	(Other harm categories)	Combined Impact Level
Damage to mission delivery	L / M / H	L / M / H	L / M / H	
Damage to trust or reputation	L / M / H	L / M / H	L / M / H	
Loss of sensitive information	L / M / H	L / M / H	L / M / H	
Damage to or loss of economic stability	L / M / H	L / M / H	L / M / H	
Loss of life or damage to safety, health, or environmental stability	L / M / H	L / M / H	L / M / H	
Noncompliance with laws, regulations, and/or contractual obligations	L / M / H	L / M / H	L / M / H	

1167 The output of this step is a defined impact level for failures of identity proofing,
 1168 authentication, and federation which serve as the primary input to the initial assurance
 1169 level selection.

1170 **5.2. Select Initial Assurance Levels**

1171 The impact analysis serves as a primary input to the process of selecting initial assurance
 1172 levels for identity proofing, authentication and federation. The assurance levels may differ
 1173 across these areas based on the analysis of the potential impact of failures in each area.
 1174 The purpose of these initial assurance levels is to identify baseline digital identity controls
 1175 and processes, reflected in the requirements and guidelines in the companion volumes of
 1176 [SP800-63A], [SP800-63B], and [SP800-63C], which will be assessed and tailored based
 1177 on mission need, cybersecurity risk, and other potential impacts to the organization and
 1178 users of the digital identity systems.

1179 **5.2.1. Assurance Levels**

1180 An organization RP **SHALL** select, based on cybersecurity risk and mission needs, the
1181 following individual initial assurance levels:

- 1182 • **IAL**: The robustness of the identity proofing process to confidently determine the
1183 identity of an individual. IAL is selected to mitigate potential identity proofing
1184 failures.
- 1185 • **AAL**: The robustness of the authentication process itself, and the binding between
1186 an authenticator and a specific individual's identifier. AAL is selected to mitigate
1187 potential authentication failures.
- 1188 • **FAL**: The robustness of the federation process used to communicate authentication
1189 and attribute information (if applicable) to an RP from an IdP. FAL is optional as
1190 not all digital systems will leverage federated identity architectures. FAL is selected
1191 to mitigate potential federation failures.

1192 **5.2.2. xAL Descriptions**

1193 A summary of each of the identity, authenticator, and federation assurance levels is
1194 provided below.

1195 When described generically or bundled, these guidelines will refer to IAL, AAL, and FAL
1196 as *xAL*.

1197 **5.2.2.1. Identity Assurance Level**

1198 **IAL1**: IAL1 requires validation of identifying attributes against authoritative or credible
1199 sources and use of basic processes to verify the claimed identity of the applicant.

1200 **IAL2**: IAL2 requires identifying attributes to be supported by strong evidence and
1201 validated against authoritative or credible sources and use of processes to verify the
1202 claimed identity of the applicant.

1203 **IAL3**: IAL3 requires identifying attributes to be verified by an authorized CSP
1204 representative through examination of physical documentation using an interactive
1205 process with a CSP representative.

1206 **5.2.2.2. Authentication Assurance Level**

1207 **AAL1**: AAL1 provides some assurance that the claimant controls an authenticator
1208 registered to the subscriber. AAL1 requires single-factor authentication using a wide
1209 range of available authentication technologies. Successful authentication requires that the
1210 claimant prove possession and control of the authenticator through a secure authentication
1211 protocol.

1212 **AAL2**: AAL2 provides high confidence that the claimant controls authenticator registered
1213 to the subscriber. Proof of possession and control of two different authentication factors is

1214 required through a secure authentication protocol. Approved cryptographic techniques are
1215 required at AAL2 and above.

1216 **AAL3:** AAL3 provides very high confidence that the claimant controls authenticator
1217 registered to the subscriber. Authentication at AAL3 is based on proof of possession of a
1218 key through a cryptographic authentication protocol capable of resisting phishing attacks.

1219 **5.2.2.3. Federation Assurance Level**

1220 **FAL1:** FAL1 allows for the subscriber to log into the RP using an assertion from the
1221 IdP that can be verified by the RP as coming from the IdP and targeted for a specific RP.
1222 The assertion is protected from modification or construction by an attacker. The trust
1223 agreement and registration between the IdP and RP can happen dynamically.

1224 **FAL2:** FAL2 adds the requirement that the assertion be robust against injection at the
1225 RP. One means of this is to have the assertion presented directly to the RP from the IdP
1226 instead of passing through an intermediary like a browser. The trust agreement between
1227 the IdP and RP cannot happen dynamically, but dynamic registration of the specific IdP
1228 and RP can occur at runtime.

1229 **FAL3:** FAL3 adds the requirement that the subscriber authenticate directly to the RP
1230 using a bound authenticator along with presenting the authentication assertion. The
1231 presence of this additional authenticator provides a very high assurance to the RP that
1232 the party accessing the RP is the party identified in the assertion. The trust agreement and
1233 registration cannot be dynamic.

1234 **5.2.3. Initial Assurance Level Selection**

1235 The identification and assessment of the potential impacts of failures in identity proofing,
1236 authentication, and federation processes informs the organization's digital identity risk
1237 management process and the initial selection of assurance levels for those areas. These
1238 initial selections are primarily based on cybersecurity risk, but will be tailored, based on
1239 mission needs and other potential impacts to the organization, users, and mission partners.

1240 Organizations **SHALL** develop and document a process and governance model for
1241 selecting initial assurance levels based on the potential impact of digital identity failures.
1242 This section provides guidance on the major elements to include in that process.

1243 **5.2.3.1. Selecting Initial IAL**

1244 The IAL reflects the level of assurance that an applicant holds the claimed real-life
1245 identity. Organizations **SHALL** use a risk-based approach to select the most appropriate
1246 identity proofing requirements for their RP application. The impact analysis described in
1247 **Sec. 5.3.1** informs the selection of the initial IAL selection. This initial selection **SHALL**
1248 be tailored, as described in **Sec. 5.3**, based on mission needs, risk tolerance, and potential
1249 impacts to privacy, equity, and usability, before making a final IAL determination.

1250 The IAL selection does not mean the RP application owner will need to perform the
1251 proofing themselves since identity proofing is the function of the CSP.

1252 Not all RP applications will require identity proofing. If the RP application does not
1253 require any personal information to execute any digital transactions, the system can
1254 operate without identity proofing users of the RP application. If personal information
1255 is needed, the RP needs to determine if validated and verified attributes are required or
1256 if self-asserted attributes are acceptable. If there are insignificant potential harms from
1257 accepting self-asserted attributes, the system may also be able to operate without identity
1258 proofing users. In such cases, the identity proofing processes described in [SP800-63A]
1259 are not applicable to the system.

1260 If an organization determines that identity proofing is necessary, the initial IAL
1261 **SHALL** be assessed based on the potential impacts of identity proofing failures. As
1262 described in [Sec. 5.1](#), potential impacts **SHALL** be considered from the perspective of
1263 the organization, individuals, other organizations, and the nation, for harms incurred
1264 through the use or operation of the RP application. While the organization may not be
1265 negatively impacted, the user could be significantly harmed, as could individuals whose
1266 privacy or other rights have been violated by the business practices of a service provider.
1267 Organizations **SHOULD** consider the worst-case when identifying the overall impact
1268 level of the RP application, but may use risk management processes to tailor their initial
1269 selection when there are differing impacts.

1270 When assessing the overall impact level of the RP application, the organization **SHOULD**
1271 consider impacts to mission delivery separately from other impact categories. Potential
1272 failures in the identity proofing process that could lead to harms in mission delivery
1273 should be assessed by the organization to determine if the associated impacts would
1274 be mitigated or exacerbated by the implementation of more rigorous identity proofing
1275 processes. As such, the organization **MAY** exclude the mission delivery category when
1276 initially identifying the overall impact level of the RP application, as these impacts will
1277 need to be considered in the tailoring process.

1278 The overall impact level assessed by the organization leads to a preliminary selection of
1279 the IAL from which further tailoring may be done:

- 1280 • Low impact: IAL1
- 1281 • Moderate impact: IAL2
- 1282 • High impact: IAL3

1283 The preliminary selection assumes that higher potential impacts of failures in the identity
1284 proofing process should be mitigated by higher assurance processes. While this is often
1285 the case, organizations should consider the specific failures, impact categories, and
1286 impacted entities identified as part of the impact analysis to determine if additional
1287 tailoring is warranted. For example, if a failure to enroll a legitimate applicant could lead

1288 to excessive harm, organizations should assess whether lower-assurance identity proofing
1289 processes would be appropriate.

1290 The result of this process, including any additional tailoring, is the initial assessment
1291 of the IAL, which will be assessed against additional potential impacts as described in
1292 [Sec. 5.3](#).

1293 **5.2.3.2. Selecting Initial AAL**

1294 The AAL reflects the level of assurance from the authentication process that the claimant
1295 is who they claim to be. Organizations **SHALL** use a risk-based approach to select
1296 the most appropriate authentication requirements for their RP application. The impact
1297 analysis described in [Sec. 5.1.3](#) informs the selection of the initial AAL selection. This
1298 initial selection **SHALL** be tailored, as described in [Sec. 5.3](#), based on mission needs, risk
1299 tolerance, and potential impacts to privacy, equity, and usability, before making a final
1300 AAL determination.

1301 The AAL selection does not mean the RP application owner will need to issue
1302 authenticators themselves.

1303 The initial AAL **SHALL** be assessed based on the potential impacts of authentication
1304 failures. As described in [Sec. 5.1](#), potential impacts **SHALL** be considered from the
1305 perspective of the organization, individuals, other organizations, and the nation, for harms
1306 incurred through the use or operation of the RP application, as the level of harm from a
1307 failure could vary significantly across these entities. Organizations **SHOULD** consider
1308 the worst-case when identifying the overall impact level of the RP application, but may
1309 use risk management processes to tailor their initial selection when there are differing
1310 impacts.

1311 When assessing the overall impact level of the RP application, the organization **SHOULD**
1312 consider impacts to mission delivery separately from other impact categories. Potential
1313 failures in the authentication process that could lead to harms in mission delivery should
1314 be assessed by the organization to determine if the associated impacts would be mitigated
1315 or exacerbated by the implementation of more rigorous authentication controls. As such,
1316 the organization **MAY** exclude the mission delivery category when initially identifying
1317 the overall impact level of the RP application, as these impacts will need to be considered
1318 in the tailoring process.

1319 The overall impact level assessed by the organization leads to a preliminary selection of
1320 the AAL from which further tailoring may be done:

- 1321 • Low impact: AAL1
- 1322 • Moderate impact: AAL2
- 1323 • High impact: AAL3

1324 The preliminary selection assumes that higher potential impacts of failures in the
1325 authentication process should be mitigated by higher assurance processes. While this
1326 is often the case, organizations should consider the specific failures, impact categories,
1327 and impacted entities identified as part of the impact analysis to determine if additional
1328 tailoring is warranted. Further, organizations should consider legal, regulatory, or
1329 policy requirements that govern digital services. For example, the terms of [EO13681]
1330 requiring “that all organizations making personal data accessible to citizens through
1331 digital applications require the use of multiple factors of authentication,” which would
1332 drive the selection of AAL2 or AAL3.

1333 The result of this process, including any additional tailoring, is the initial assessment of
1334 the AAL, which will be as assessed against additional potential impacts as described in
1335 [Sec. 5.3](#).

1336 **5.2.3.3. Selecting Initial FAL**

1337 The FAL reflects the level of assurance in identity assertions that convey the results of
1338 authentication processes and relevant identity information to RP systems. Organizations
1339 **SHALL** use a risk-based approach to select the most appropriate federation requirements
1340 for their RP application. The impact analysis described in [Sec. 5.3.1](#) informs the selection
1341 of the initial FAL selection. This initial selection **SHALL** be tailored, as described in
1342 [Sec. 5.3](#), based on mission needs, risk tolerance, and potential impacts to privacy, equity,
1343 and usability, before making a final FAL determination.

1344 The initial FAL **SHALL** be assessed based on the potential impacts of failures in the
1345 presentation or acceptance of assertions in federated identity architectures. Examples
1346 of compromise include use of assertion replay to impersonate a valid user or leakage of
1347 assertion information through the browser. As described in [Sec. 5.1](#), potential impacts
1348 **SHALL** be considered from the perspective of the organization, individuals, other
1349 organizations, and the nation, for harms incurred through the use or operation of the
1350 RP application, as the level of harm from a failure could vary significantly across these
1351 entities. Organizations **SHOULD** consider the worst-case when identifying the overall
1352 impact level of the RP application, but may use risk management processes to tailor their
1353 initial selection when there are differing impacts.

1354 When assessing the overall impact level of the RP application, the organization **SHOULD**
1355 consider impacts to mission delivery separately from other impact categories. Potential
1356 failures in federated architectures that could lead to harms in mission delivery **MAY** be
1357 assessed by the organization to determine if the associated impacts would be mitigated or
1358 exacerbated by the implementation of more rigorous controls by identity providers. As
1359 such, the organization may exclude the mission delivery impact category when initially
1360 identifying the overall impact level of the RP application, as these impacts will need to be
1361 considered in the tailoring process.

1362 The overall impact level assessed by the organization leads to a preliminary selection of
1363 the FAL from which further tailoring may be done:

- 1364 • Low impact: FAL1
- 1365 • Moderate impact: FAL2
- 1366 • High impact: FAL3

1367 The preliminary selection assumes that higher potential impacts of failures in federated
1368 identity architectures should be mitigated by higher assurance processes. While this is
1369 often the case, organizations should consider the specific failures, impact categories,
1370 and impacted entities identified as part of the impact analysis to determine if additional
1371 tailoring is warranted.

1372 The result of this process, including any additional tailoring, is the initial assessment of
1373 the FAL, which will be as assessed against additional potential impacts as described in
1374 [Sec. 5.3](#).

1375 **5.3. Tailor and Document Assurance Levels**

1376 Tailoring provides a process to modify an initially assessed assurance level or implement
1377 compensating controls based on ongoing detailed impact and risk assessments.

1378 Organizations **SHOULD** implement the assessed assurance level as defined in these
1379 guidelines. However, these guidelines provide flexibility to allow for organizations
1380 to meet specific mission needs and address unique risk appetites and considerations.
1381 Therefore, organizations **SHALL** establish and document an xAL tailoring process. At a
1382 minimum this process:

- 1383 1. **SHALL** include a structured governance approach to allow for decision-making
1384 and conflict resolution.
- 1385 2. **SHALL** document all decisions in the tailoring process, including the assessed
1386 xALs, modified xALs, and compensating controls in the Digital Identity
1387 Acceptance Statement (see [Sec. 5.3.4](#)).
- 1388 3. **SHALL** justify and document all risk-based decisions or modifications to
1389 the initially assessed xALs in the Digital Identity Acceptance Statement (see
1390 [Sec. 5.3.4](#)).
- 1391 4. **SHOULD** establish a cross-functional capability to support subject matter analysis
1392 of xAL selection impacts in the tailoring process.
- 1393 5. **SHOULD** be a continuous process that incorporates real world operational data to
1394 evaluate the impacts of selected xAL controls.

1395 The tailoring process promotes a structured means to balance risks and impacts in the
1396 furtherance of protecting systems, data, and services in a manner that enables mission
1397 success while supporting equity, privacy, and usability for individuals.

1398 **5.3.1. Assess Privacy, Equity, Usability and Threats**

1399 When selecting and tailoring assurance levels for specific applications, it is critical that
1400 insights and inputs to the process extend beyond an initial, static impact assessment.

1401 When transitioning from an initial assurance level to the final xAL selection and
1402 implementation, organizations **SHALL** conduct detailed assessments of the controls
1403 defined at the assurance level to determine potential impacts in their operational
1404 environment. At a minimum, organizations **SHALL** assess impacts related to the
1405 following areas:

- 1406 • **Privacy** – to determine unintended consequences to the privacy of individuals that
1407 will be subject to the controls at an assessed xAL and of individuals affected by
1408 organizational or third-party practices related to the establishment, management, or
1409 federation of a digital identity.
- 1410 • **Equity** – to determine whether implementation of controls may create or maintain
1411 inequities across demographics or user groups.
- 1412 • **Usability** – to determine whether implementation of the selected controls will result
1413 in challenges to end-user experience.
- 1414 • **Threat** – to determine whether the defined assurance level will address specific
1415 threats based on environment, threat actors, and known tactics, techniques, and
1416 procedures (TTPs).

1417 Additionally, organizations **SHOULD** conduct additional business specific assessments
1418 as appropriate to fully represent mission and domain specific considerations not captured
1419 here. These assessments **SHALL** be extended to any compensating or supplemental
1420 controls as defined in [Sec. 5.3.2](#) and [Sec. 5.3.3](#).

1421 **5.3.2. Identify Compensating Controls**

1422 A compensating control is a management, operational, or technical control employed
1423 by an organization in lieu of a recommended control in the defined xALs. They are
1424 intended, to the greatest degree possible, to address the same risks as the baseline control
1425 is intended to address.

1426 Organizations **SHOULD** implement their identity services per the requirements in these
1427 guidelines for their tailored assurance level. However, where organizations are unable
1428 to implement a specific control associated with their baseline or tailored assurance
1429 level, they **MAY** select to implement a compensating control. This control **MAY** be a
1430 modification to a digital identity process as defined in these guidelines, but **MAY** also be
1431 applied elsewhere in an application, transaction, or service lifecycle. For example:

- 1432 • A federal agency could choose to use a federal background investigation and
1433 checks, as referenced by *Personal Identity Verification [FIPS201]*, to compensate
1434 for the identity evidence validation with authoritative sources requirement under
1435 these guidelines.

- 1436 • An organization could choose to implement stricter auditing and transactional
1437 review processes on a payment application where verification processes using
1438 weaker forms of identity evidence were accepted due to availability of evidence
1439 in the end-user population.

1440 Where compensating controls are implemented, organizations **SHALL** demonstrate
1441 comparability of a chosen alternative or document residual risk incurred by deviating
1442 from normative requirements. Organizations **SHALL** implement procedures to document
1443 both the justification for any departure from normative requirements and detail the
1444 compensating controls employed. The inclusion of compensating controls does not
1445 imply that an organization must tailor to a lower xAL. The process of tailoring allows
1446 for agencies and service providers to make risk-based decisions in how they implement
1447 their xALs and provides a mechanism for documenting and communicating decisions
1448 through the Digital Identity Acceptance Statement described in [Sec. 5.3.4](#).

1449 **5.3.3. Identify Supplemental Controls**

1450 Supplemental controls are those that may be added, in addition to those specified in the
1451 organizations tailored assurance level, in order to address specific threats or attacks.
1452 Organizations **SHOULD** identify and implement supplemental controls where they
1453 identify threats that may not be addressed in baseline controls. For example:

- 1454 • An organization could choose to verify an end user against additional pieces of
1455 identity evidence, beyond what is required by the assurance level, due to a high
1456 prevalence of fraudulent attempts to complete the proofing process.
- 1457 • An organization could choose to implement risk-scoring analytics, coupled with
1458 re-proofing mechanisms, to confirm a user's identity when their access attempts
1459 exhibit certain risk factors.

1460 Where organizations implement supplemental controls, these **SHALL** be assessed for
1461 impacts based on the same factors used to tailor the organization's assurance level.
1462 Supplemental controls **SHALL** be documented.

1463 **5.3.4. Document Results - The Digital Identity Acceptance Statement**

1464 The Digital Identity Acceptance Statement documents the results of the digital identity
1465 risk management process. This includes the Impact Assessment, Initial Assurance Level
1466 Selection, and Tailoring process.

1467 The statement **SHALL** include, at a minimum:

- 1468 1. Initial Impact Assessment Results
- 1469 2. Initially assessed xAL,
- 1470 3. Tailored xAL and rationale, if tailored xAL differs from initially assessed xAL,

1471 4. All compensating controls and their comparability or residual risk associated with
1472 compensating controls

1473 5. All supplemental controls

1474 Federal agencies **SHOULD** include this information in the system authorization package
1475 described in [SP800-37].

1476 **5.4. Continuously Evaluate and Improve**

1477 Threat actors adapt, user expectations and needs shift, and missions evolve. As such,
1478 risk assessments and identity solutions are not to be set and forgotten. To maintain pace
1479 with the constantly shifting environment in which they operate, organizations **SHOULD**
1480 implement a continuous evaluation and improvement program that leverages input from
1481 people interacting with the identity system. These programs **SHOULD** consider feedback
1482 from application performance metrics, threat intelligence, fraud analytics, assessments of
1483 equity impacts, privacy impact analysis, and user inputs.

1484 **5.5. Cyber, Fraud, and Identity Program Integrity**

1485 Typically, identity solutions are the front door for a critical business or service function.
1486 Accordingly, they should not operate in a vacuum. Close coordination of identity
1487 functions with cybersecurity teams, threat intelligence teams, and program integrity
1488 teams can enable a more complete protection of business capabilities, while constantly
1489 improving identity solution capabilities. For example, payment fraud data collected
1490 by program integrity teams could provide indicators of compromised subscriber
1491 accounts and potential weaknesses in identity proofing implementations. Similarly,
1492 threat intelligence teams may receive indication of new TTPs that may impact identity
1493 proofing, authentication, and federation processes. Organizations **SHOULD** establish
1494 consistent mechanisms for the exchange of information between critical security and
1495 fraud stakeholders.

1496 Where supporting service providers, such as CSPs, are external, this may be complicated,
1497 but **SHOULD** be considered in contractual and legal mechanisms. All data collected,
1498 transmitted, or shared **SHALL** be minimized and subject to a detailed privacy and legal
1499 assessment.

1500 **References**

1501 *This section is informative.*

1502 **General References**

1503 **[A-130]** OMB Circular A-130, *Managing Federal Information as a Strategic Resource*,
1504 July 28, 2016, available at: [https://obamawhitehouse.archives.gov/sites/default/files/omb/
1505 assets/OMB/circulars/a130/a130revised.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf).

1506 **[EO13681]** Executive Order 13681, *Improving the Security of Consumer Financial
1507 Transactions*, October 17, 2014, available at: [https://www.federalregister.gov/d/2014-
1508 25439](https://www.federalregister.gov/d/2014-25439).

1509 **[EO13985]** Executive Order 13985, *Advancing Racial Equity and Support for
1510 Underserved Communities Through the Federal Government*, January 25, 2021, available
1511 at: [https://www.federalregister.gov/documents/2021/01/25/2021-01753/advancing-racial-
1512 equity-and-support-for-underserved-communities-through-the-federal-government](https://www.federalregister.gov/documents/2021/01/25/2021-01753/advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government)

1513 **[FISMA]** *Federal Information Security Modernization Act of 2014*, 44 U.S.C. § 3551
1514 *et seq.*, Public Law (P.L.) 113-283, available at: [https://www.congress.gov/bill/113th-
1515 congress/senate-bill/2521](https://www.congress.gov/bill/113th-congress/senate-bill/2521).

1516 **[M-03-22]** OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy
1517 Provisions of the E-Government Act of 2002*, September 26, 2003, available at: [https:
1518 //georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html](https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html).

1519 **[NISTIR8062]** NIST Internal Report 8062, *An Introduction to Privacy Engineering and
1520 Risk Management in Federal Systems*, January 2017, available at: [https://nvlpubs.nist.gov/
1521 nistpubs/ir/2017/NIST.IR.8062.pdf](https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf).

1522 **[NISTRMF]** *Risk Management Framework Overview*, available at [https://csrc.nist.gov/
1523 groups/SMA/fisma/framework.html](https://csrc.nist.gov/groups/SMA/fisma/framework.html).

1524 **[NISTPF]** *NIST Privacy Framework*, available at [https://www.nist.gov/privacy-
1525 framework/privacy-framework](https://www.nist.gov/privacy-framework/privacy-framework).

1526 **[PrivacyAct]** *The Privacy Act of 1974*, available at [https://www.govinfo.gov/content/pkg/
1527 USCODE-2020-title5/pdf/USCODE-2020-title5-partI-chap5-subchapII-sec552a.pdf](https://www.govinfo.gov/content/pkg/USCODE-2020-title5/pdf/USCODE-2020-title5-partI-chap5-subchapII-sec552a.pdf)

1528 **[SORN]** United States Office of Personnel Management (OPM), *System of Records
1529 Notice (SORN) Guide*, April 22, 2010, available at: [https://www.opm.gov/information-
1530 management/privacy-policy/privacy-references/sornguide.pdf](https://www.opm.gov/information-management/privacy-policy/privacy-references/sornguide.pdf)

1531 **Standards**

1532 **[BCP195]** Sheffer, Y., Holz, R., and P. Saint-Andre, *Recommendations for Secure Use*
1533 *of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*,
1534 BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, available at: <https://doi.org/10.17487/RFC7525>.
1535

1536 **[ISO9241-11]** International Standards Organization, *ISO/IEC 9241-11 Ergonomic*
1537 *requirements for office work with visual display terminals (VDTs) — Part 11: Guidance*
1538 *on usability*, March 1998, available at: <https://www.iso.org/standard/16883.html>.

1539 **[OIDC]** Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore,
1540 *OpenID Connect Core 1.0 incorporating errata set 1*, December, 2014. Available at:
1541 <https://openid.net/specs/openid-connect-core-1.0.html>.

1542 **[RFC5246]** Dierks, T. and E. Rescorla, *The Transport Layer Security (TLS) Protocol*
1543 *Version 1.2*, RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.
1544

1545 **[RFC5280]** Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W.
1546 Polk, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation*
1547 *List (CRL) Profile*, RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.
1548

1549 **NIST Special Publications**

1550 NIST 800 Series Special Publications are available at: < <https://csrc.nist.gov/publications/sp8001>>.
1551 The following publications may be of particular interest to those implementing systems of
1552 applications requiring digital authentication.

1553 **[SP800-30]** NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk*
1554 *Assessments*, September 2012, available at: <https://doi.org/10.6028/NIST.SP.800-30r1>.

1555 **[SP800-37]** NIST Special Publication 800-37 Revision 2, *Risk Management Framework*
1556 *for Information Systems and Organizations: A System Life Cycle Approach for Security*
1557 *and Privacy*, December 2018, available at: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>.
1558

1559 **[SP800-52]** NIST Special Publication 800-52 Revision 2, *Guidelines for the Selection,*
1560 *Configuration, and Use of Transport Layer Security (TLS) Implementations*, August 2019,
1561 available at: <https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final>.

1562 **[SP800-53]** NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls*
1563 *for Information Systems and Organizations*, September 2020 (includes updates as of Dec.
1564 10, 2020), available at: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>.

1565 **[SP800-53A]** NIST Special Publication 800-53A Revision 5, *Assessing Security and*
1566 *Privacy Controls in Information Systems and Organizations*, January 2022, available at:

1567 <https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final>.

1568 **[SP800-57Part1]** NIST Special Publication 800-57 Part 1, Revision 5, *Recommendation*
1569 *for Key Management, Part 1: General*, May 2020, [https://dx.doi.org/10.6028/NIST.SP.](https://dx.doi.org/10.6028/NIST.SP.800-57pt1r5)
1570 [800-57pt1r5](https://dx.doi.org/10.6028/NIST.SP.800-57pt1r5).

1571 **[SP800-63A]** NIST Special Publication 800-63B-4, *Digital Identity Guidelines:*
1572 *Enrollment and Identity Proofing*, December 2022, [https://doi.org/10.6028/](https://doi.org/10.6028/NIST.SP.800-63a-4.ipd)
1573 [NIST.SP.800-63a-4.ipd](https://doi.org/10.6028/NIST.SP.800-63a-4.ipd).

1574 **[SP800-63B]** NIST Special Publication 800-63B-4, *Digital Identity Guidelines:*
1575 *Authentication and Lifecycle Management*, November 2022, [https://doi.org/10.6028/](https://doi.org/10.6028/NIST.SP.800-63b-4.ipd)
1576 [NIST.SP.800-63b-4.ipd](https://doi.org/10.6028/NIST.SP.800-63b-4.ipd).

1577 **[SP800-63C]** NIST Special Publication 800-63C-4, *Digital Identity Guidelines:*
1578 *Assertions and Federation*, November 2022, [https://doi.org/10.6028/](https://doi.org/10.6028/NIST.SP.800-63c-4.ipd)
1579 [NIST.SP.800-63c-4.ipd](https://doi.org/10.6028/NIST.SP.800-63c-4.ipd).

1580 **Federal Information Processing Standards**

1581 **[FIPS199]** Federal Information Processing Standard 199, *Standards for Security*
1582 *Categorization of Federal Information and Information Systems*, February 2004, available
1583 at: <https://doi.org/10.6028/NIST.FIPS.199>.

1584 **[FIPS201]** Federal Information Processing Standard Publication 201-3, *Personal Identity*
1585 *Verification (PIV) of Federal Employees and Contractors*, January 2022, available at:
1586 <https://csrc.nist.gov/publications/detail/fips/201/3/final>.

1587 **Appendix A. Definitions and Abbreviations**

1588 *This section is informative.*

1589 **A.1. Definitions**

1590 A wide variety of terms is used in the realm of authentication. While many terms'
1591 definitions are consistent with earlier versions of SP 800-63, some have changed in this
1592 revision. Many of these terms lack a single, consistent definition, warranting careful
1593 attention to how the terms are defined here.

1594 **Access**

1595 To make contact with one or more discrete functions of an online, digital service.

1596 **Activation**

1597 The process of inputting an *activation factor* into a *multi-factor authenticator* to enable its
1598 use for *authentication*.

1599 **Activation factor**

1600 An additional *authentication factor* that is used to enable successful *authentication*
1601 with a *multi-factor authenticator*. Since all multi-factor authenticators are physical
1602 authenticators, activation factors are either *memorized secrets* or *biometric* factors.

1603 **Active Attack**

1604 An attack on the authentication protocol where the attacker transmits data to the claimant,
1605 Credential Service Provider (CSP), verifier, or Relying Party (RP). Examples of active
1606 attacks include attacker-in-the-middle (AitM), impersonation, and session hijacking.

1607 **Address of Record**

1608 The validated and verified location (physical or digital) where a subscriber can receive
1609 communications using approved mechanisms.

1610 **Allowlist**

1611 A documented list of specific elements that are allowed, per policy decision. In federation
1612 contexts, this is most commonly used to refer to the list of RPs allowed to connect to
1613 an IdP without subscriber intervention. This concept has historically been known as a
1614 *whitelist*.

1615 **Applicant**

1616 A subject undergoing the processes of enrollment and identity proofing.

1617 **Approved Cryptography**

1618 Federal Information Processing Standard (FIPS)-approved or NIST recommended. An
1619 algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or
1620 2) adopted in a FIPS or NIST Recommendation.

1621 **Assertion**

1622 A statement from a verifier to an RP that contains information about a subscriber.
1623 Assertions may also contain verified attributes.

1624 **Assertion Reference**

1625 A data object, created in conjunction with an assertion, that identifies the verifier and
1626 includes a pointer to the full assertion held by the verifier.

1627 **Asymmetric Keys**

1628 Two related keys, comprised of a public key and a private key, that are used to perform
1629 complementary operations such as encryption and decryption or signature verification and
1630 generation.

1631 **Attack**

1632 An unauthorized entity's attempt to fool a verifier or RP into believing that the
1633 unauthorized individual in question is the subscriber.

1634 **Attacker**

1635 A party, including an insider, who acts with malicious intent to compromise a system.

1636 **Attacker-in-the-Middle Attack (AitM)**

1637 An attack in which an attacker is positioned between two communicating parties in order
1638 to intercept and/or alter data traveling between them. In the context of authentication, the
1639 attacker would be positioned between claimant and verifier, between registrant and CSP
1640 during enrollment, or between subscriber and CSP during authenticator binding.

1641 **Attribute**

1642 A quality or characteristic ascribed to someone or something.

1643 **Attribute API**

1644 An API that provides *attribute values*, *derived attribute values*, and related information
1645 about one or more subscribers. Access to these APIs are often granted to RPs in the
1646 context of an *identity API* (for a single subscriber) or a *provisioning API* (for multiple
1647 subscribers). This is distinct from an *attribute verification API* which is used to verify
1648 attribute values for a CSP during the identity proofing process.

1649 **Attribute Bundle**

1650 A packaged set of attributes, usually contained within an assertion. Attribute bundles offer
1651 RPs a simple way to retrieve the most relevant attributes they need from IdPs. OpenID
1652 Connect scopes [OIDC] are an implementation of attribute bundles.

1653 **Attribute Provider**

1654 A service that provides a subscriber's attributes without asserting that the subscriber is
1655 present to the RP. An *Identity Provider (IdP)* is one type of attribute provider used in
1656 federated scenarios. Attribute providers often make these attributes available by means of
1657 an *attribute API*.

1658 **Attribute Value**

1659 A complete statement asserting a property of a subscriber, independent of format. For
1660 example, for the attribute "birthday," a value could be "12/1/1980" or "December 1,
1661 1980."

1662 **Attribute Verification API**

1663 An API that provides verification of *attribute values* for use during an *identity proofing*
1664 process. This API accepts attribute values as input queries and returns whether or not the
1665 attribute values can be verified. This is distinct from an *attribute API* which is used to
1666 convey attributes to an RP.

1667 **Authenticate**

1668 See [Authentication](#).

1669 **Authenticated Protected Channel**

1670 An encrypted communication channel that uses approved cryptography where the
1671 connection initiator (client) has authenticated the recipient (server). Authenticated
1672 protected channels provide confidentiality and MitM protection and are frequently used in
1673 the user authentication process. Transport Layer Security (TLS) [BCP195] is an example
1674 of an authenticated protected channel where the certificate presented by the recipient is
1675 verified by the initiator. Unless otherwise specified, authenticated protected channels
1676 do not require the server to authenticate the client. Authentication of the server is often
1677 accomplished through a certificate chain leading to a trusted root rather than individually
1678 with each server.

1679 **Authentication**

1680 The process of determining the validity of one or more authenticators used to claim a
1681 digital identity. Authentication establishes that a subject attempting to access a digital
1682 service is in control of the technologies used to authenticate.

1683 **Authentication Factor**

1684 The three types of authentication factors are *something you know*, *something you have*,
1685 and *something you are*. Every authenticator has one or more authentication factors.

1686 **Authentication Intent**

1687 The process of confirming the claimant’s intent to authenticate or reauthenticate
1688 by including a process requiring user intervention in the authentication flow. Some
1689 authenticators (e.g., OTP devices) establish authentication intent as part of their operation,
1690 others require a specific step, such as pressing a button, to establish intent. Authentication
1691 intent is a countermeasure against use by malware of the endpoint as a proxy for
1692 authenticating an attacker without the subscriber’s knowledge.

1693 **Authentication Protocol**

1694 A defined sequence of messages between a claimant and a verifier that demonstrates that
1695 the claimant has possession and control of one or more valid authenticators to establish
1696 their identity, and, optionally, demonstrates that the claimant is communicating with the
1697 intended verifier.

1698 **Authentication Secret**

1699 A generic term for any secret value that an attacker could use to impersonate the
1700 subscriber in an authentication protocol.

1701 These are further divided into *short-term authentication secrets*, which are only useful
1702 to an attacker for a limited period of time, and *long-term authentication secrets*, which
1703 allow an attacker to impersonate the subscriber until they are manually reset. The
1704 authenticator secret is the canonical example of a long-term authentication secret, while
1705 the authenticator output, if it is different from the authenticator secret, is usually a short-
1706 term authentication secret.

1707 **Authenticator**

1708 Something the claimant possesses and controls (typically a cryptographic module or
1709 password) that is used to authenticate the claimant’s identity. In some previous editions of
1710 SP 800-63, this was referred to as a *token*.

1711 **Authentication Assurance Level (AAL)**

1712 A category describing the strength of the authentication process.

1713 **Authenticator Output**

1714 The output value generated by an authenticator. The ability to generate valid authenticator
1715 outputs on demand proves that the claimant possesses and controls the authenticator.
1716 Protocol messages sent to the verifier are dependent upon the authenticator output, but
1717 they may or may not explicitly contain it.

1718 **Authenticator Secret**

1719 The secret value contained within an authenticator.

1720 **Authenticator Type**

1721 A category of authenticators with common characteristics. Some authenticator types
1722 provide one authentication factor, others provide two.

1723 **Authenticity**

1724 The property that data originated from its purported source.

1725 **Authoritative Source**

1726 An entity that has access to, or verified copies of, accurate information from an issuing
1727 source such that a CSP can confirm the validity of the identity evidence supplied by an
1728 applicant during identity proofing. An issuing source may also be an authoritative source.
1729 Often, authoritative sources are determined by a policy decision of the agency or CSP
1730 before they can be used in the identity proofing validation phase.

1731 **Authorize**

1732 A decision to grant [access](#), typically automated by evaluating a subject's attributes.

1733 **Authorized Party**

1734 In federation, the organization, person, or entity that is responsible for making decisions
1735 regarding the release of information within the federation transaction, most notably
1736 subscriber attributes. This is often the subscriber (when runtime decisions are used) or
1737 the party operating the IdP (when allowlists are used).

1738 **Back-Channel Communication**

1739 Communication between two systems that relies on a direct connection (allowing for
1740 standard protocol-level proxies), without using redirects through an intermediary such as
1741 a browser. This can be accomplished using HTTP requests and responses.

1742 **Bearer Assertion**

1743 The assertion a party presents as proof of identity, where possession of the assertion itself
1744 is sufficient proof of identity for the assertion bearer.

1745 **Binding**

1746 An association between a subscriber identity and an authenticator or given subscriber
1747 session.

1748 **Biometric Reference**

1749 one or more stored biometric samples, templates, or models attributed to an individual
1750 and used as the object of biometric comparison. For example, a facial image stored
1751 digitally on a passport, fingerprint minutiae template on a National ID card or Gaussian
1752 Mixture Model for speaker recognition, in a database.

1753 **Biometric Sample**

1754 An analog or digital representation of biometric characteristics prior to biometric feature
1755 extraction. An example is a record containing a fingerprint image.

1756 **Biometrics**

1757 Automated recognition of individuals based on their biological and behavioral
1758 characteristics.

1759 **Blocklist**

1760 A documented list of specific elements that are blocked, per policy decision. This concept
1761 has historically been known as a *blacklist*.

1762 **Challenge-Response Protocol**

1763 An authentication protocol where the verifier sends the claimant a challenge (usually a
1764 random value or nonce) that the claimant combines with a secret (such as by hashing
1765 the challenge and a shared secret together, or by applying a private key operation
1766 to the challenge) to generate a response that is sent to the verifier. The verifier can
1767 independently verify the response generated by the claimant (such as by re-computing the
1768 hash of the challenge and the shared secret and comparing to the response, or performing
1769 a public key operation on the response) and establish that the claimant possesses and
1770 controls the secret.

1771 **Claimant**

1772 A subject whose identity is to be verified using one or more authentication protocols.

1773 **Claimed Address**

1774 The physical location asserted by a subject where they can be reached. It includes the
1775 individual's residential street address and may also include their mailing address.

1776 For example, a person with a foreign passport living in the U.S. will need to give an
1777 address when going through the identity proofing process. This address would not be
1778 an "address of record" but a "claimed address."

1779 **Claimed Identity**

1780 An applicant's declaration of unvalidated and unverified personal attributes.

1781 **Completely Automated Public Turing test to tell Computers and Humans Apart
1782 (CAPTCHA)**

1783 An interactive feature added to web forms to distinguish whether a human or automated
1784 agent is using the form. Typically, it requires entering text corresponding to a distorted
1785 image or a sound stream.

1786 **Core Attributes**

1787 The set of identity attributes the CSP has determined and documented to be required for
1788 identity proofing.

1789 **Credential**

1790 An object or data structure that authoritatively binds an identity - via an identifier or
1791 identifiers - and (optionally) additional attributes, to at least one authenticator possessed
1792 and controlled by a subscriber.

1793 A credential is issued, stored, and maintained by the CSP. Copies of information from
1794 the credential can be possessed by the subscriber, typically in the form of a one or more
1795 digital certificates that are often contained, along with their associated private keys, in an
1796 authenticator.

1797 **Credential Service Provider (CSP)**

1798 A trusted entity whose functions include identity proofing applicants to the identity
1799 service and the registration of authenticators to subscriber accounts. A CSP may be an
1800 independent third party.

1801 **Cross-site Request Forgery (CSRF)**

1802 An attack in which a subscriber currently authenticated to an RP and connected through
1803 a secure session browses to an attacker's website, causing the subscriber to unknowingly
1804 invoke unwanted actions at the RP.

1805 For example, if a bank website is vulnerable to a CSRF attack, it may be possible for
1806 a subscriber to unintentionally authorize a large money transfer, merely by viewing a
1807 malicious link in a webmail message while a connection to the bank is open in another
1808 browser window.

1809 **Cross-site Scripting (XSS)**

1810 A vulnerability that allows attackers to inject malicious code into an otherwise benign
1811 website. These scripts acquire the permissions of scripts generated by the target website
1812 and can therefore compromise the confidentiality and integrity of data transfers between
1813 the website and client. Websites are vulnerable if they display user-supplied data from
1814 requests or forms without sanitizing the data so that it is not executable.

1815 **Cryptographic Authenticator**

1816 An authenticator that proves possession of an authentication secret through direct
1817 communication, via the endpoint, with a verifier.

1818 **Cryptographic Key**

1819 A value used to control cryptographic operations, such as decryption, encryption,
1820 signature generation, or signature verification. For the purposes of these guidelines,

1821 key requirements shall meet the minimum requirements stated in Table 2 of NIST
1822 [SP800-57Part1].

1823 See also Asymmetric Keys, Symmetric Key.

1824 **Cryptographic Module**

1825 A set of hardware, software, and/or firmware that implements approved security functions
1826 (including cryptographic algorithms and key generation).

1827 **Data Integrity**

1828 The property that data has not been altered by an unauthorized entity.

1829 **Derived Attribute Value**

1830 A statement asserting a property of a subscriber without necessarily containing identity
1831 information, independent of format. For example, instead of requesting the attribute
1832 “birthday,” a derived value could be “older than 18”. Instead of requesting the attribute for
1833 “physical address,” a derived value could be “currently residing in this district.” Previous
1834 versions of these guidelines referred to this construct as an “attribute reference”.

1835 **Digital Authentication**

1836 The process of establishing confidence in user identities presented digitally to a system.
1837 In previous editions of SP 800-63, this was referred to as *Electronic Authentication*.

1838 **Digital Signature**

1839 An asymmetric key operation where the private key is used to digitally sign data and
1840 the public key is used to verify the signature. Digital signatures provide authenticity
1841 protection, integrity protection, and non-repudiation, but not confidentiality protection.

1842 **Disassociability**

1843 Per [NISTIR8062]: The processing of PII or events without association to individuals or
1844 devices beyond the operational requirements of the system.

1845 **Eavesdropping Attack**

1846 An attack in which an attacker listens passively to the authentication protocol to capture
1847 information that can be used in a subsequent active attack to masquerade as the claimant.

1848 **Electronic Authentication (E-Authentication)**

1849 See *Digital Authentication*.

1850 **Enrollment**

1851 The process through which an applicant applies to become a subscriber of a CSP and the
1852 CSP validates the applicant’s identity.

1853 **Entropy**

1854 A measure of the amount of uncertainty an attacker faces to determine the value of a
1855 secret. Entropy is usually stated in bits. A value having n bits of entropy has the same
1856 degree of uncertainty as a uniformly distributed n -bit random value.

1857 **Equity**

1858 Per EO 13985, Equity refers to the consistent and systematic fair, just, and impartial
1859 treatment of all individuals, including individuals who belong to underserved
1860 communities that have been denied such treatment, such as Black, Latino, and Indigenous
1861 and Native American persons, Asian Americans and Pacific Islanders, and other persons
1862 of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer
1863 (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons
1864 otherwise adversely affected by persistent poverty or inequality.

1865 **Federal Information Processing Standard (FIPS)**

1866 Under the Information Technology Management Reform Act (Public Law 104-106),
1867 the Secretary of Commerce approves the standards and guidelines that the National
1868 Institute of Standards and Technology (NIST) develops for federal computer systems.
1869 NIST issues these standards and guidelines as Federal Information Processing Standards
1870 (FIPS) for government-wide use. NIST develops FIPS when there are compelling federal
1871 government requirements, such as for security and interoperability, and there are no
1872 acceptable industry standards or solutions. See background information for more details.

1873 FIPS documents are available online on the FIPS home page: <https://www.nist.gov/itl/fips.cfm>
1874 [cfm](https://www.nist.gov/itl/fips.cfm)

1875 **Federated Identifier**

1876 The combination of a *subject identifier* within an assertion and an identifier for the *IdP*
1877 that issued that assertion. When combined, these pieces of information uniquely identify
1878 the *subscriber* in the context of a *federation transaction*.

1879 **Federation**

1880 A process that allows the conveyance of identity and authentication information across a
1881 set of networked systems.

1882 **Federation Assurance Level (FAL)**

1883 A category describing the assertion protocol used by the federation to communicate
1884 authentication and attribute information (if applicable) to an RP.

1885 **Federation Proxy**

1886 A component that acts as a logical RP to a set of IdPs and a logical IdP to a set of RPs,
1887 bridging the two systems with a single component. These are sometimes referred to as
1888 “brokers”.

1889 **Federation Transaction**

1890 A specific instance of processing an authentication using a *federation* process for a
1891 specific *subscriber* by conveying an *assertion* from an *IdP* to an *RP*.

1892 **Front-Channel Communication**

1893 Communication between two systems that relies on redirects through an intermediary
1894 such as a browser. This is normally accomplished by appending HTTP query parameters
1895 to URLs hosted by the receiver of the message.

1896 **Hash Function**

1897 A function that maps a bit string of arbitrary length to a fixed-length bit string. Approved
1898 hash functions satisfy the following properties:

- 1899 1. One-way - It is computationally infeasible to find any input that maps to any pre-
1900 specified output; and
- 1901 2. Collision resistant - It is computationally infeasible to find any two distinct inputs
1902 that map to the same output.

1903 **Identity**

1904 An attribute or set of attributes that uniquely describe a subject within a given context.

1905 **Identity API**

1906 An *attribute API* accessed by an *RP* for accessing attributes of a specific subscriber.
1907 Access to the identity API is generally granted as part of a federation authentication
1908 process and limited to the information for a single, specific subscriber.

1909 **Identity Assurance Level (IAL)**

1910 A category that conveys the degree of confidence that the applicant's claimed identity is
1911 their real identity.

1912 **Identity Evidence**

1913 Information or documentation provided by the applicant to support the claimed identity.
1914 Identity evidence may be physical (e.g. a driver license) or digital (e.g. an assertion
1915 generated and issued by a CSP based on the applicant successfully authenticating to the
1916 CSP).

1917 **Identity Proofing**

1918 The process by which a CSP collects, validates, and verifies information about a person.

1919 **Identity Provider (IdP)**

1920 When using federation, this is the party that manages the subscriber's primary
1921 authenticators and issues assertions derived from the subscriber account.

1922 **Identity Resolution**

1923 The process of collecting information about an applicant in order to uniquely distinguish
1924 an individual within the context of the population the CSP serves.

1925 **Issuing Source**

1926 An authority responsible for the generation of data, digital evidence (such as assertions),
1927 or physical documents that can be used as identity evidence.

1928 **Kerberos**

1929 A widely used authentication protocol developed at MIT. In “classic” Kerberos, users
1930 share a secret password with a Key Distribution Center (KDC). The user (Alice) who
1931 wishes to communicate with another user (Bob) authenticates to the KDC and the KDC
1932 furnishes a “ticket” to use to authenticate with Bob.

1933 See [SP800-63C] Sec. 11.2 for more information.

1934 **Knowledge-Based Verification (KBV)**

1935 Identity verification method based on knowledge of private information associated with
1936 the claimed identity. This is often referred to as knowledge-based authentication (KBA)
1937 or knowledge-based proofing (KBP).

1938 **Manageability**

1939 Per NISTIR 8062: Providing the capability for granular administration of personally
1940 identifiable information, including alteration, deletion, and selective disclosure.

1941 **Memorized Secret**

1942 A type of authenticator comprised of a character string intended to be memorized or
1943 memorable by the subscriber, permitting the subscriber to demonstrate *something they*
1944 *know* as part of an authentication process.

1945 **Message Authentication Code (MAC)**

1946 A cryptographic checksum on data that uses a symmetric key to detect both accidental
1947 and intentional modifications of the data. MACs provide authenticity and integrity
1948 protection, but not non-repudiation protection.

1949 **Mobile Code**

1950 Executable code that is normally transferred from its source to another computer system
1951 for execution. This transfer is often through the network (e.g., JavaScript embedded in a
1952 web page) but may transfer through physical media as well.

1953 **Multi-Factor**

1954 A characteristic of an authentication system or an authenticator that requires more than
1955 one distinct **authentication factor** for successful authentication. MFA can be performed
1956 using a single authenticator that provides more than one factor or by a combination of
1957 authenticators that provide different factors.

1958 The three authentication factors are something you know, something you have, and
1959 something you are.

1960 **Multi-Factor Authentication (MFA)**

1961 An authentication system that requires more than one distinct **authentication factor** for
1962 successful authentication. Multi-factor authentication can be performed using a multi-
1963 factor authenticator or by a combination of authenticators that provide different factors.

1964 The three authentication factors are *something you know*, *something you have*, and
1965 *something you are*.

1966 **Multi-Factor Authenticator**

1967 An authenticator that provides more than one distinct authentication factor, such as a
1968 cryptographic authentication device with an integrated biometric sensor that is required to
1969 activate the device.

1970 **Network**

1971 An open communications medium, typically the Internet, used to transport messages
1972 between the claimant and other parties. Unless otherwise stated, no assumptions are
1973 made about the network's security; it is assumed to be open and subject to active
1974 (e.g., impersonation, attacker-in-the-middle, session hijacking) and passive (e.g.,
1975 eavesdropping) attack at any point between the parties (e.g., claimant, verifier, CSP, RP).

1976 **Nonce**

1977 A value used in security protocols that is never repeated with the same key. For example,
1978 nonces used as challenges in challenge-response authentication protocols must not be
1979 repeated until authentication keys are changed. Otherwise, there is a possibility of a
1980 replay attack. Using a nonce as a challenge is a different requirement than a random
1981 challenge, because a nonce is not necessarily unpredictable.

1982 **Offline Attack**

1983 An attack where the attacker obtains some data (typically by eavesdropping on an
1984 authentication transaction or by penetrating a system and stealing security files) that
1985 the attacker is able to analyze in a system of their own choosing.

1986 **One-to-one (1:1) Comparison**

1987 The process in which a biometric sample from an individual is compared to a biometric
1988 reference to produce a comparison score.

1989 **Online Attack**

1990 An attack against an authentication protocol where the attacker either assumes the role of
1991 a claimant with a genuine verifier or actively alters the authentication channel.

1992 **Online Guessing Attack**

1993 An attack in which an attacker performs repeated logon trials by guessing possible values
1994 of the authenticator output.

1995 **Pairwise Pseudonymous Identifier**

1996 An opaque unguessable subscriber identifier generated by a CSP for use at a specific
1997 individual RP. This identifier is only known to and only used by one CSP-RP pair.

1998 **Passive Attack**

1999 An attack against an authentication protocol where the attacker intercepts data traveling
2000 along the network between the claimant and verifier, but does not alter the data (i.e.,
2001 eavesdropping).

2002 **Passphrase**

2003 A passphrase is a memorized secret consisting of a sequence of words or other text that a
2004 claimant uses to authenticate their identity. A passphrase is similar to a password in usage,
2005 but is generally longer for added security.

2006 **Password**

2007 See *memorized secret*.

2008 **Personal Data**

2009 See *Personally Identifiable Information*.

2010 **Personal Identification Number (PIN)**

2011 A memorized secret typically consisting of only decimal digits.

2012 **Personal Information**

2013 See *Personally Identifiable Information*.

2014 **Personally Identifiable Information (PII)**

2015 As defined by [OMB Circular A-130](#), PII is information that can be used to distinguish or
2016 trace an individual's identity, either alone or when combined with other information that
2017 is linked or linkable to a specific individual.

2018 **Personally Identifiable Information Processing**

2019 An operation or set of operations performed upon personally identifiable information
2020 that can include, but is not limited to, the collection, retention, logging, generation,

2021 transformation, use, disclosure, transfer, and disposal of personally identifiable
2022 information.

2023 **Pharming**

2024 An attack in which an attacker corrupts an infrastructure service such as DNS (Domain
2025 Name System) causing the subscriber to be misdirected to a forged verifier/RP, which
2026 could cause the subscriber to reveal sensitive information, download harmful software, or
2027 contribute to a fraudulent act.

2028 **Phishing**

2029 An attack in which the subscriber is lured (usually through an email) to interact with
2030 a counterfeit verifier/RP and tricked into revealing information that can be used to
2031 masquerade as that subscriber to the real verifier/RP.

2032 **Possession and Control of an Authenticator**

2033 The ability to activate and use the authenticator in an authentication protocol.

2034 **Practice Statement**

2035 A formal statement of the practices followed by the parties to an authentication process
2036 (e.g., CSP or verifier). It usually describes the parties' policies and practices and can
2037 become legally binding.

2038 **Predictability**

2039 Per [NISTIR8062]: Enabling reliable assumptions by individuals, owners, and operators
2040 about PII and its processing by an information system.

2041 **Private Key**

2042 The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.

2043 **Processing**

2044 Per [NISTIR8062]: Operation or set of operations performed upon PII that can include,
2045 but is not limited to, the collection, retention, logging, generation, transformation, use,
2046 disclosure, transfer, and disposal of PII.

2047 **Presentation Attack**

2048 Presentation to the biometric data capture subsystem with the goal of interfering with the
2049 operation of the biometric system.

2050 **Presentation Attack Detection (PAD)**

2051 Automated determination of a presentation attack. A subset of presentation attack
2052 determination methods, referred to as *liveness detection*, involves measurement and
2053 analysis of anatomical characteristics or involuntary or voluntary reactions, in order to

2054 determine if a biometric sample is being captured from a living subject present at the
2055 point of capture.

2056 **Protected Session**

2057 A session wherein messages between two participants are encrypted and integrity is
2058 protected using a set of shared secrets called session keys.

2059 A protected session is said to be *authenticated* if, during the session, one participant
2060 proves possession of one or more authenticators in addition to the session keys, and if the
2061 other party can verify the identity associated with the authenticator(s). If both participants
2062 are authenticated, the protected session is said to be *mutually authenticated*.

2063 **Provisioning API**

2064 An *attribute API* that allows an RP to access to attributes for multiple subscribers for
2065 the purposes of provisioning RP subscriber accounts. Access to a provisioning API is
2066 generally granted to the RP outside of a specific federated authentication transaction.

2067 **Pseudonym**

2068 A name other than a legal name.

2069 **Pseudonymity**

2070 The use of a pseudonym to identify a subject.

2071 **Pseudonymous Identifier**

2072 A meaningless but unique number that does not allow the RP to infer anything regarding
2073 the subscriber but which does permit the RP to associate multiple interactions with the
2074 subscriber's claimed identity.

2075 **Public Key**

2076 The public part of an asymmetric key pair that is used to verify signatures or encrypt data.

2077 **Public Key Certificate**

2078 A digital document issued and digitally signed by the private key of a certificate authority
2079 that binds an identifier to a subscriber to a public key. The certificate indicates that the
2080 subscriber identified in the certificate has sole control and access to the private key. See
2081 also [\[RFC5280\]](#).

2082 **Public Key Infrastructure (PKI)**

2083 A set of policies, processes, server platforms, software, and workstations used for the
2084 purpose of administering certificates and public-private key pairs, including the ability to
2085 issue, maintain, and revoke public key certificates.

2086 **Reauthentication**

2087 The process of confirming the subscriber's continued presence and intent to be
2088 authenticated during an extended usage session.

2089 **Registration**

2090 See [Enrollment](#).

2091 **Relying Party (RP)**

2092 An entity that relies upon a verifier's assertion of a subscriber's identity, typically to
2093 process a transaction or grant access to information or a system.

2094 **Remote**

2095 *(In the context of remote authentication or remote transaction)* An information exchange
2096 between network-connected devices where the information cannot be reliably protected
2097 end-to-end by a single organization's security controls.

2098 **Replay Attack**

2099 An attack in which the attacker is able to replay previously captured messages (between
2100 a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or vice
2101 versa.

2102 **Replay Resistance**

2103 The property of an authentication process to resist replay attacks, typically by use of an
2104 authenticator output that is valid only for a specific authentication.

2105 **Resolution**

2106 See *Identity Resolution*.

2107 **Restricted**

2108 An authenticator type, class, or instantiation having additional risk of false acceptance
2109 associated with its use that is therefore subject to additional requirements.

2110 **Risk Assessment**

2111 The process of identifying, estimating, and prioritizing risks to organizational operations
2112 (including mission, functions, image, or reputation), organizational assets, individuals,
2113 and other organizations, resulting from the operation of a system. It is part of risk
2114 management, incorporates threat and vulnerability analyses, and considers mitigations
2115 provided by security controls planned or in place. Synonymous with risk analysis.

2116 **Risk Management**

2117 The program and supporting processes to manage information security risk to
2118 organizational operations (including mission, functions, image, reputation), organizational

2119 assets, individuals, other organizations, and includes: (i) establishing the context for risk-
2120 related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv)
2121 monitoring risk over time.

2122 **Salt**

2123 A non-secret value used in a cryptographic process, usually to ensure that the results of
2124 computations for one instance cannot be reused by an attacker.

2125 **Secure Sockets Layer (SSL)**

2126 See *Transport Layer Security (TLS)*.

2127 **Session**

2128 A persistent interaction between a subscriber and an endpoint, either an RP or a CSP. A
2129 session begins with an authentication event and ends with a session termination event.
2130 A session is bound by use of a session secret that the subscriber's software (a browser,
2131 application, or OS) can present to the RP to prove association of the session with the
2132 authentication event.

2133 **Session Hijack Attack**

2134 An attack in which the attacker is able to insert themselves between a claimant and a
2135 verifier subsequent to a successful authentication exchange between the latter two parties.
2136 The attacker is able to pose as a subscriber to the verifier or vice versa to control session
2137 data exchange. Sessions between the claimant and the RP can be similarly compromised.

2138 **Shared Secret**

2139 A secret used in authentication that is known to the subscriber and the verifier.

2140 **Side-Channel Attack**

2141 An attack enabled by leakage of information from a physical cryptosystem.
2142 Characteristics that could be exploited in a side-channel attack include timing, power
2143 consumption, and electromagnetic and acoustic emissions.

2144 **Single-Factor**

2145 A characteristic of an authentication system or an authenticator that requires only one
2146 authentication factor (something you know, something you have, or something you are)
2147 for successful authentication.

2148 **Social Engineering**

2149 The act of deceiving an individual into revealing sensitive information, obtaining
2150 unauthorized access, or committing fraud by associating with the individual to gain
2151 confidence and trust.

2152 **Software Statement**

2153 **Software Statement**

2154 A list of attributes describing a piece of software that is cryptographically signed by an
2155 authority. Software statements are used most commonly with RPs in a federated scenario.

2156 **Special Publication (SP)**

2157 A type of publication issued by NIST. Specifically, the SP 800-series reports on the
2158 Information Technology Laboratory's research, guidelines, and outreach efforts in
2159 computer security, and its collaborative activities with industry, government, and
2160 academic organizations.

2161 **Subject**

2162 A person, organization, device, hardware, network, software, or service.

2163 **Subscriber**

2164 An individual enrolled in the CSP identity service.

2165 **Subscriber Account**

2166 An account established by the CSP containing information and authenticators registered
2167 for each subscriber enrolled in the CSP identity service.

2168 **Supervised Remote Identity Proofing**

2169 A remote identity proofing process that employs physical, technical and procedural
2170 measures that provide sufficient confidence that the remote session can be considered
2171 equivalent to a physical, in-person identity proofing process.

2172 **Symmetric Key**

2173 A cryptographic key used to perform both the cryptographic operation and its inverse. For
2174 example, to encrypt and decrypt or create a message authentication code and to verify the
2175 code.

2176 **Synthetic identity fraud**

2177 The use of a combination of personally identifiable information (PII) to fabricate a person
2178 or entity in order to commit a dishonest act for personal or financial gain.

2179 **Token**

2180 See [Authenticator](#).

2181 **Transaction**

2182 A discrete event between a user and a system that supports a business or programmatic
2183 purpose. A government digital system may have multiple categories or types of

2184 transactions, which may require separate analysis within the overall digital identity risk
2185 assessment.

2186 **Transport Layer Security (TLS)**

2187 An authentication and security protocol widely implemented in browsers and web servers.
2188 TLS is defined by [RFC5246]. TLS is similar to the older SSL protocol, and TLS 1.0 is
2189 effectively SSL version 3.1. NIST SP 800-52, Guidelines for the Selection and Use of
2190 Transport Layer Security (TLS) Implementations [SP800-52], specifies how TLS is to be
2191 used in government applications.

2192 **Trust Anchor**

2193 A public or symmetric key that is trusted because it is directly built into hardware or
2194 software, or securely provisioned via out-of-band means, rather than because it is vouched
2195 for by another trusted entity (e.g. in a public key certificate). A trust anchor may have
2196 name or policy constraints limiting its scope.

2197 **Usability**

2198 The extent to which a product can be used by specified users to achieve specified
2199 goals with effectiveness, efficiency, and satisfaction in a specified context of use.
2200 [ISO/IEC9241-11]

2201 **Validation**

2202 The process or act of checking and confirming that the evidence and attributes supplied by
2203 an applicant are authentic, accurate and associated with a real-life identity. Specifically,
2204 evidence validation is the process or act of checking that presented evidence is authentic,
2205 current, and issued from an acceptable source; attribute validation is the process or act of
2206 confirming the a set of attributes are accurate and associated with a real-life identity.

2207 **Verification**

2208 The process or act of confirming that the applicant holds the claimed identity represented
2209 by the validated identity attributes and associated evidence. In NIST SP 800-63, the term
2210 “verification” is synonymous with “identity verification.”

2211 **Verifier**

2212 An entity that verifies the claimant’s identity by verifying the claimant’s possession and
2213 control of one or more authenticators using an authentication protocol. To do this, the
2214 verifier needs to confirm the binding of the authenticators with the subscriber account and
2215 check that the subscriber account is active.

2216 **Verifier Impersonation**

2217 See [Phishing](#).

2218 **Zeroize**

2219 Overwrite a memory location with data consisting entirely of bits with the value zero
2220 so that the data is destroyed and not recoverable. This is often contrasted with deletion
2221 methods that merely destroy reference to data within a file system rather than the data
2222 itself.

2223 **Zero-Knowledge Password Protocol**

2224 A password-based authentication protocol that allows a claimant to authenticate to a
2225 verifier without revealing the password to the verifier. Examples of such protocols are
2226 EKE, SPEKE and SRP.

2227 **A.2. Abbreviations**

2228 Selected abbreviations in these guidelines are defined below.

2229 **ABAC**

2230 Attribute Based Access Control

2231 **AAL**

2232 Authentication Assurance Level

2233 **CAPTCHA**

2234 Completely Automated Public Turing test to tell Computer and Humans Apart

2235 **CSP**

2236 Credential Service Provider

2237 **CSRF**

2238 Cross-site Request Forgery

2239 **XSS**

2240 Cross-site Scripting

2241 **DNS**

2242 Domain Name System

2243 **EO**

2244 Executive Order

2245 **FACT Act**

2246 Fair and Accurate Credit Transaction Act of 2003

2247	FAL
2248	Federation Assurance Level
2249	FEDRAMP
2250	Federal Risk and Authorization Management Program
2251	FMR
2252	False Match Rate
2253	FNMR
2254	False Non-Match Rate
2255	FIPS
2256	Federal Information Processing Standard
2257	FISMA
2258	Federal Information Security Modernization Act
2259	1:1 Comparison
2260	One-to-one Comparison
2261	IAL
2262	Identity Assurance Level
2263	IdP
2264	Identity Provider
2265	IoT
2266	Internet of Things
2267	ISO/IEC
2268	International Organization for Standardization/International Electrotechnical Commission
2269	JOSE
2270	JSON Object Signing and Encryption
2271	JSON
2272	JavaScript Object Notation
2273	JWT
2274	JSON Web Token

2275	KBA
2276	Knowledge-Based Authentication
2277	KBV
2278	Knowledge-Based Verification
2279	KDC
2280	Key Distribution Center
2281	LOA
2282	Level of Assurance
2283	MAC
2284	Message Authentication Code
2285	MFA
2286	Multi-Factor Authentication
2287	N/A
2288	Not Applicable
2289	NARA
2290	National Archives and Records Administration
2291	OMB
2292	Office of Management and Budget
2293	OTP
2294	One-Time Password
2295	PAD
2296	Presentation Attack Detection
2297	PIA
2298	Privacy Impact Assessment
2299	PII
2300	Personally Identifiable Information
2301	PIN
2302	Personal Identification Number

- 2303 **PKI**
- 2304 Public Key Infrastructure

- 2305 **PL**
- 2306 Public Law

- 2307 **PSTN**
- 2308 Public Switched Telephone Network

- 2309 **RMF**
- 2310 Risk Management Framework

- 2311 **RP**
- 2312 Relying Party

- 2313 **SA&A**
- 2314 Security Authorization & Accreditation

- 2315 **SAML**
- 2316 Security Assertion Markup Language

- 2317 **SAOP**
- 2318 Senior Agency Official for Privacy

- 2319 **SSL**
- 2320 Secure Sockets Layer

- 2321 **SMS**
- 2322 Short Message Service

- 2323 **SP**
- 2324 Special Publication

- 2325 **SORN**
- 2326 System of Records Notice

- 2327 **TEE**
- 2328 Trusted Execution Environment

- 2329 **TGS**
- 2330 Ticket Granting Server

- 2331 **TGT**
- 2332 Ticket Granting Ticket

- 2333 **TLS**
- 2334 Transport Layer Security

- 2335 **TPM**
- 2336 Trusted Platform Module

- 2337 **TTP**
- 2338 Tactics, Techniques, and Procedures

- 2339 **VOIP**
- 2340 Voice-over-IP

2341 **Appendix B. Change Log**

2342 **B.1. SP 800-63-1**

2343 NIST SP 800-63-1 updated NIST SP 800-63 to reflect current authenticator (then referred
2344 to as “token”) technologies and restructured it to provide a better understanding of
2345 the digital identity architectural model used here. Additional (minimum) technical
2346 requirements were specified for the CSP, protocols used to transport authentication
2347 information, and assertions if implemented within the digital identity model.

2348 **B.2. SP 800-63-2**

2349 NIST SP 800-63-2 was a limited update of SP 800-63-1 and substantive changes were
2350 made only in Sec. 5, *Registration and Issuance Processes*. The substantive changes in the
2351 revised draft were intended to facilitate the use of professional credentials in the identity
2352 proofing process, and to reduce the need to send postal mail to an address of record to
2353 issue credentials for level 3 remote registration. Other changes to Sec. 5 were minor
2354 explanations and clarifications.

2355 **B.3. SP 800-63-3**

2356 NIST SP 800-63-3 is a substantial update and restructuring of SP 800-63-2. SP 800-63-
2357 3 introduces individual components of digital authentication assurance — AAL, IAL,
2358 and FAL — to support the growing need for independent treatment of authentication
2359 strength and confidence in an individual’s claimed identity (e.g., in strong pseudonymous
2360 authentication). A risk assessment methodology and its application to IAL, AAL, and
2361 FAL has been included in this guideline. It also moves the whole of digital identity
2362 guidance covered under SP 800-63 from a single document describing authentication
2363 to a suite of four documents (to separately address the individual components mentioned
2364 above) of which SP 800-63-3 is the top-level document.

2365 Other areas updated in 800-63-3 include:

- 2366 • Renamed to *Digital Identity Guidelines* to properly represent the scope includes
2367 identity proofing and federation, and to support expanding the scope to include
2368 device identity, or machine-to-machine authentication in future revisions.
- 2369 • Changed terminology, including the use of *authenticator* in place of *token* to avoid
2370 conflicting use of the word *token* in assertion technologies.
- 2371 • Updated authentication and assertion requirements to reflect advances in both
2372 security technology and threats.
- 2373 • Added requirements on the storage of long-term secrets by verifiers.
- 2374 • Restructured identity proofing model.
- 2375 • Updated requirements regarding remote identity proofing.

- 2376 • Clarified the use of independent channels and devices as “something you have”.
- 2377 • Removed pre-registered knowledge tokens (authenticators), with the recognition
2378 that they are special cases of (often very weak) passwords.
- 2379 • Added requirements regarding account recovery in the event of loss or theft of an
2380 authenticator.
- 2381 • Removed email as a valid channel for out-of-band authenticators.
- 2382 • Expanded discussion of reauthentication and session management.
- 2383 • Expanded discussion of identity federation; restructuring of assertions in the
2384 context of federation.

2385 **B.4. SP 800-63-4**

2386 NIST SP 800-63-4 has substantial updates and re-organization from SP 800-63-3.
2387 Updates to 800-63-4 include:

- 2388 • **Section 2.3** expands security and privacy consideration content of previous
2389 revisions. It also adds equity and usability considerations.
- 2390 • **Section 4.1** includes updated non-federated and federated digital identity models
2391 and descriptions.
- 2392 • **Section 4.4** consolidates informative descriptions and considerations on the use of
2393 federated identity architectures and assertions into one section.
- 2394 • **Section 5** expands upon the risk management content of previous revisions and
2395 specifically mandates that organizations take into account impacts to individuals
2396 and communities in addition to impacts to the organization. It also elevates risks
2397 to mission delivery, including challenges to the provisioning of services to all
2398 people who are eligible for and entitled to them, within the risk management
2399 process and when implementing digital identity systems. The xAL selection
2400 flowcharts, previously found in 800-63-3, section 6, have been replaced with text
2401 that elaborates the risk management process along with a sample risk assessment
2402 matrix that supports xAL selection. Additionally, the guidelines now mandate
2403 continuous evaluation of potential impacts to individuals, communities, and
2404 organizations.