

COMMONWEALTH OF VIRGINIA



~~Information Technology Resource
Management~~ **IDENTITY MANAGEMENT STANDARDS
ADVISORY COUNCIL (ITRM/IMSAC)**

GUIDANCE DOCUMENT

~~Federation and Participant Requirements~~ **Electronic Authentication**

~~Virginia Information Technologies Agency (VITA)~~

Table of Contents

1	Publication Version Control	1
2	Reviews	1
<u>3</u>	<u>Purpose and Scope</u>	<u>1</u>
3-4	Statutory Authority	2
4-5	Definitions	3
5-6	Background	14-15
6-7	Minimum Specifications	15-16
7	Alignment Comparison	26

Formatted: Font: 5 pt

DRAFT

1 Publication Version Control

The following table contains a history of revisions to this publication.

Publication Version	Date	Revision Description
1.0	<u>07/2010/12</u> /2016	Initial Draft of Document

Formatted Table

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) for the Secretary of Technology, under the direction from the Identity Management Standards Advisory Council (IMSAC). The initial version of the document was prepared by the staff analysts for the Identity Management Standards Advisory Council, within Commonwealth Data Governance, Enterprise Architecture, Virginia Information Technologies Agency.
- The document will be reviewed in a manner compliant with the Commonwealth of Virginia's Administrative Process Act, § 2.2-4000 et seq.

Formatted: List Paragraph, Indent: Left: 0", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Normal, No bullets or numbering

Formatted: List Paragraph, Indent: Left: 0", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0"

3 Purpose and Scope

- Pursuant to § 2.2-436 and § 2.2-437, Code of Virginia, this guidance document was developed by the Identity Management Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to establish minimum specifications for Digital Identity Systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), Chapter 50 of Title 59.1. The guidance document, as defined in § 2.2-4001, was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. The guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive

Formatted: Normal, No bullets or numbering

32 ~~branch agencies of the Commonwealth of Virginia. The document will be reviewed in a manner~~
33 ~~compliant with the Commonwealth of Virginia’s ITRM Policies, Standards, and Guidelines and~~
34 ~~§2.2-437-C, Code of Virginia:~~

35
36 ~~Proposed guidance documents and general opportunity for oral or written submittals as to~~
37 ~~those guidance documents shall be posted on the Virginia Regulatory Town Hall and published~~
38 ~~in the Virginia Register of Regulations as a general notice following the processes and~~
39 ~~procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act~~
40 ~~(§2.2-4000 et seq.). The Advisory Council [IMSAC] shall allow at least 30 days for the submission~~
41 ~~of written comments following the posting and publication and shall hold at least one meeting~~
42 ~~dedicated to the receipt of oral comment no less than 15 days after the posting and publication.~~
43 ~~The Advisory Council shall also develop methods for the identification and notification of~~
44 ~~interested parties and specific means of seeking input from interested persons and groups. The~~
45 ~~Advisory Council shall send a copy of such notices, comments, and other background material~~
46 ~~relative to the development of the recommended guidance documents to the Joint Commission~~
47 ~~on Administrative Rules.~~

Formatted: Indent: Left: 0"

50 **3.4 Statutory Authority**

51
52 The following section documents the statutory authority established in the *Code of Virginia* for
53 the development of minimum specifications and standards for Federation and Participant
54 Requirements in a Digital Identity System. References to statutes below and throughout this
55 document shall be to the *Code of Virginia*, unless otherwise specified.

56
57 **Governing Statutes:**

58
59 **Secretary of Technology**

60 § 2.2-225. Position established; agencies for which responsible; additional powers
61 <http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/>

62
63 **Identity Management Standards Advisory Council**

64 § 2.2-437. Identity Management Standards Advisory Council
65 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/>

66
67 **Commonwealth Identity Management Standards**

68 § 2.2-436. Approval of electronic identity standards
69 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/>

70
71 **Electronic Identity Management Act**

72 Chapter 50. Electronic Identity Management Act
73 <http://law.lis.virginia.gov/vacode/title59.1/chapter50/>

74
75 The following section documents the statutory authority established in the *Code of Virginia* for
76 the development of minimum specifications and standards for electronic authentication.
77 References to statutes below and throughout this document shall be to the *Code of Virginia*,
78 unless otherwise specified.

79
80 **Governing Statutes:**

81
82 **Secretary of Technology**

83 § 2.2-225. Position established; agencies for which responsible; additional powers
84 <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225>

85
86 **Secretary of Transportation**

87 § 2.2-225. Position established; agencies for which responsible; additional powers
88 <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225>

89

90 **Identity Management Standards Advisory Council**

91 § 2.2-437. Identity Management Standards Advisory Council

92 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/>

93

94 **Commonwealth Identity Management Standards**

95 § 2.2-436. Approval of electronic identity standards

96 <http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/>

97

98 **Electronic Identity Management Act**

99 Chapter 50. Electronic Identity Management Act

100 <http://law.lis.virginia.gov/vacode/title59.1/chapter50/>

101

102 **Chief Information Officer (CIO) of the Commonwealth**

103 § 2.2-2007. Powers of the CIO

104 <http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2007>

105

106 **Virginia Information Technologies Agency**

107 § 2.2-2010. Additional powers of VITA

108 <http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2010>

109

110

111

112

113

114

115 **45 Definitions**

116
117 Terms used in this document comply with definitions in the Public Review version of the
118 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3),
119 and align with adopted definitions in § 59.1-550, Code of Virginia (COV), and the
120 Commonwealth of Virginia’s ITRM Glossary (ITRM Glossary).¹
121
122 Active Attack: An online attack where the attacker transmits data to the claimant, credential
123 service provider, verifier, or relying Participant. Examples of active attacks include man-in-the-
124 middle, impersonation, and session hijacking.
125
126 Address of Record: The official location where an individual can be found. The address of record
127 always includes the residential street address of an individual and may also include the mailing
128 address of the individual. In very limited circumstances, an Army Post Office box number, Fleet
129 Post Office box number or the street address of next of kin or of another contact individual can
130 be used when a residential street address for the individual is not available.
131
132 Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An
133 algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2)
134 adopted in a FIPS or NIST Recommendation.
135
136 Applicable Law: Laws, statutes, regulations, and rules of the jurisdiction in which the members
137 of an Identity Trust Framework operates.
138
139 Applicant: A Participant undergoing the processes of Registration and Identity Proofing.
140
141 Assertion: A statement from a verifier to a relying Participant (RP) that contains identity
142 information about a Subscriber. Assertions may also contain verified attributes.
143
144 Assertion Reference: A data object, created in conjunction with an Assertion, which identifies
145 the verifier and includes a pointer to the full Assertion held by the verifier.
146
147 Assurance: In the context of [OMB M-04-04]² and this document, assurance is defined as 1) the
148 degree of confidence in the vetting process used to establish the identity of an individual to
149 whom the credential was issued, and 2) the degree of confidence that the individual who uses
150 the credential is the individual to whom the credential was issued.

¹ NIST SP 800-63-3 may be accessed at <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.

§ 59.1-550, Code of Virginia, may be accessed at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/>. The Commonwealth’s ITRM Glossary may be accessed at http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf

² [OMB M-04-04] Office of Management and Budget, Memorandum 04-04: E-Authentication Guidance for Federal Agencies, accessible at <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>.

151 [Assurance Model: Policies, processes, and protocols that define how Assurance will be](#)
152 [established in an Identity Trust Framework.](#)
153
154 [Asymmetric Keys: Two related keys, a public key and a private key that are used to perform](#)
155 [complementary operations, such as encryption and decryption or signature generation and](#)
156 [signature verification.](#)
157
158 [Attack: An attempt by an unauthorized individual to fool a verifier or a relying Participant into](#)
159 [believing that the unauthorized individual in question is the Subscriber.](#)
160
161 [Attacker: A Participant who acts with malicious intent to compromise an Information System.](#)
162
163 [Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or](#)
164 [something.](#)
165
166 [Authentication: The process of establishing confidence in the identity of users or Information](#)
167 [Systems.](#)
168
169 [Authentication Protocol: A defined sequence of messages between a claimant and a verifier](#)
170 [that demonstrates that the claimant has possession and control of a valid authenticator to](#)
171 [establish his/her identity, and optionally, demonstrates to the claimant that he or she is](#)
172 [communicating with the intended verifier.](#)
173
174 [Authentication Protocol Run: An exchange of messages between a claimant and a verifier that](#)
175 [results in authentication \(or authentication failure\) between the two Participants.](#)
176
177 [Authentication Secret: A generic term for any secret value that could be used by an attacker to](#)
178 [impersonate the Subscriber in an authentication protocol. These are further divided into short-](#)
179 [term authentication secrets, which are only useful to an attacker for a limited period of time,](#)
180 [and long-term authentication secrets, which allow an attacker to impersonate the Subscriber](#)
181 [until they are manually reset. The authenticator secret is the canonical example of a long term](#)
182 [authentication secret, while the authenticator output, if it is different from the authenticator](#)
183 [secret, is usually a short term authentication secret.](#)
184
185 [Authenticator: Something that the claimant possesses and controls \(typically a cryptographic](#)
186 [module or password\) that is used to authenticate the claimant's identity. In previous versions of](#)
187 [this guideline, this was referred to as a token.](#)
188
189 [Authenticator Assurance Level \(AAL\): A metric describing robustness of the authentication](#)
190 [process proving that the claimant is in control of a given Subscriber's authenticator\(s\).](#)
191
192 [Authenticator Output: The output value generated by an authenticator. The ability to generate](#)
193 [valid authenticator outputs on demand proves that the claimant possesses and controls the](#)

194 [authenticator. Protocol messages sent to the verifier are dependent upon the authenticator](#)
195 [output, but they may or may not explicitly contain it.](#)

196
197 [Authenticator Secret: The secret value contained within an authenticator.](#)
198 [Authenticity: The property that data originated from its purported source.](#)
199

200 [Bearer Assertion: An Assertion that does not provide a mechanism for the Subscriber to prove](#)
201 [that he or she is the rightful owner of the Assertion. The RP has to assume that the Assertion](#)
202 [was issued to the Subscriber who presents the Assertion or the corresponding Assertion](#)
203 [reference to the RP.](#)

204
205 [Bit: A binary digit: 0 or 1.](#)
206

207 [Biometrics: Automated recognition of individuals based on their behavioral and biological](#)
208 [characteristics. In this document, biometrics may be used to unlock authenticators and prevent](#)
209 [repudiation of Registration.](#)
210

211 [Certificate Authority \(CA\): A trusted entity that issues and revokes public key certificates.](#)
212

213 [Certificate Revocation List \(CRL\): A list of revoked public key certificates created and digitally](#)
214 [signed by a Certificate Authority. \[RFC 5280\]³](#)
215

216 [Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant](#)
217 [a challenge \(usually a random value or a nonce\) that the claimant combines with a secret \(such](#)
218 [as by hashing the challenge and a shared secret together, or by applying a private key operation](#)
219 [to the challenge\) to generate a response that is sent to the verifier. The verifier can](#)
220 [independently verify the response generated by the claimant \(such as by re-computing the hash](#)
221 [of the challenge and the shared secret and comparing to the response, or performing a public](#)
222 [key operation on the response\) and establish that the claimant possesses and controls the](#)
223 [secret.](#)
224

225 [Claimant: A Participant whose identity is to be verified using an authentication protocol.](#)
226 [Claimed Address: The physical location asserted by an individual \(e.g. an applicant\) where](#)
227 [he/she can be reached. It includes the residential street address of an individual and may also](#)
228 [include the mailing address of the individual. For example, a person with a foreign passport,](#)
229 [living in the U.S., will need to give an address when going through the Identity Proofing process.](#)
230 [This address would not be an “address of record” but a “claimed address.”](#)
231

232 [Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth](#)
233 [and address. \[GPG45\]⁴](#)

³ [\[RFC 5280\] Official Internet Protocol Standards, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile, May 2008, accessible at <http://www.rfc-editor.org/info/rfc5280>.](#)

234 Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA): An
235 interactive feature added to web-forms to distinguish use of the form by humans as opposed to
236 automated agents. Typically, it requires entering text corresponding to a distorted image or
237 from a sound stream.

238
239 Cookie: A character string, placed in a web browser’s memory, which is available to websites
240 within the same Internet domain as the server that placed them in the web browser.

241
242 Credential: An object or data structure that authoritatively binds an identity (and optionally,
243 additional attributes) to an authenticator possessed and controlled by a Subscriber. While
244 common usage often assumes that the credential is maintained by the Subscriber, this
245 document also uses the term to refer to electronic records maintained by the CSP which
246 establish a binding between the Subscriber’s authenticator(s) and identity.

247
248 Credential Service Provider (CSP): A trusted entity that issues or registers Subscriber
249 authenticators and issues electronic credentials to Subscribers. The CSP may encompass
250 Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third
251 Participant, or may issue credentials for its own use.

252
253 Cross Site Request Forgery (CSRF): An attack in which a Subscriber who is currently
254 authenticated to an RP and connected through a secure session, browses to an attacker’s
255 website which causes the Subscriber to unknowingly invoke unwanted actions at the RP. For
256 example, if a bank website is vulnerable to a CSRF attack, it may be possible for a Subscriber to
257 unintentionally authorize a large money transfer, merely by viewing a malicious link in a
258 webmail message while a connection to the bank is open in another browser window.

259
260 Cross Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an
261 otherwise benign website. These scripts acquire the permissions of scripts generated by the
262 target website and can therefore compromise the confidentiality and integrity of data transfers
263 between the website and client. Websites are vulnerable if they display user supplied data from
264 requests or forms without sanitizing the data so that it is not executable.

265
266 Cryptographic Key: A value used to control cryptographic operations, such as decryption,
267 encryption, signature generation or signature verification. For the purposes of this document,
268 key requirements must meet the minimum requirements stated in Table 2 of NIST SP 800-57
269 Part 1. See also Asymmetric keys, Symmetric key.

270
271 Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.
272

⁴ [GPG 45] UK Cabinet Office, Good Practice Guide 45, Identity proofing and verification of an individual, November 3, 2014, accessible at <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>.

273 [Data Integrity: The property that data has not been altered by an unauthorized entity.](#)

274

275 [Derived Credential: A credential issued based on proof of possession and control of an](#)

276 [authenticator associated with a previously issued credential, so as not to duplicate the Identity](#)

277 [Proofing process.](#)

278

279 [Digital Identity System: An Information System that supports Electronic Authentication and the](#)

280 [management of a person's Identity in a digital environment. \[Referenced in § 59.1-550, COV\]](#)

281

282 [Digital Signature: An asymmetric key operation where the private key is used to digitally sign](#)

283 [data and the public key is used to verify the signature. Digital signatures provide authenticity](#)

284 [protection, integrity protection, and non-repudiation.](#)

285

286 [Eavesdropping Attack: An attack in which an attacker listens passively to the authentication](#)

287 [protocol to capture information which can be used in a subsequent active attack to](#)

288 [masquerade as the claimant.](#)

289

290 [Electronic Authentication: The process of establishing confidence in user identities](#)

291 [electronically presented to an Information System.](#)

292

293 [Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value](#)

294 [of a secret. Entropy is usually stated in bits.](#)

295

296 [Extensible Mark-up Language \(XML\): Extensible Markup Language, abbreviated XML, describes](#)

297 [a class of data objects called XML documents and partially describes the behavior of computer](#)

298 [programs which process them.](#)

299

300 [Federal Bridge Certification Authority \(FBCA\): The FBCA is the entity operated by the Federal](#)

301 [Public Key Infrastructure \(FPKI\) Management Authority that is authorized by the Federal PKI](#)

302 [Policy Authority to create, sign, and issue public key certificates to Principal CAs.](#)

303

304 [Federal Information Security Management Act \(FISMA\): Title III of the E-Government Act](#)

305 [requiring each federal agency to develop, document, and implement an agency-wide program](#)

306 [to provide information security for the information and Information Systems that support the](#)

307 [operations and assets of the agency, including those provided or managed by another agency,](#)

308 [contractor, or other source.](#)

309

310 [Federal Information Processing Standard \(FIPS\): Under the Information Technology](#)

311 [Management Reform Act \(Public Law 104-106\), the Secretary of Commerce approves standards](#)

312 [and guidelines that are developed by the National Institute of Standards and Technology \(NIST\)](#)

313 [for Federal computer systems. These standards and guidelines are issued by NIST as Federal](#)

314 [Information Processing Standards \(FIPS\) for use government-wide. NIST develops FIPS when](#)

315 there are compelling Federal government requirements such as for security and interoperability
316 and there are no acceptable industry standards or solutions.⁵
317

318 Federation: A process that allows for the conveyance of identity and authentication information
319 across a set of networked systems. These systems are often run and controlled by disparate
320 Participants in different network and security domains. [NIST SP 800-63C]
321

322 Governance Authority: Entity responsible for providing policy level leadership, oversight,
323 strategic direction, and related governance activities within an Identity Trust Framework.
324

325 Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string.
326 Approved hash functions satisfy the following properties:

- 327 • (One-way) It is computationally infeasible to find any input that maps to any pre-
328 specified output, and
- 329 • (Collision resistant) It is computationally infeasible to find any two distinct inputs that
330 map to the same output.
331

332 Holder-of-Key Assertion: An Assertion that contains a reference to a symmetric key or a public
333 key (corresponding to a private key) held by the Subscriber. The RP may authenticate the
334 Subscriber by verifying that he or she can indeed prove possession and control of the
335 referenced key.
336

337 Identity: A set of attributes that uniquely describe a person within a given context.
338

339 Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's
340 claimed identity is their real identity.
341

342 Identity Proofing: The process by which a CSP and a Registration Authority (RA) collect and
343 verify information about a person for the purpose of issuing credentials to that person.
344

345 Identity Provider (IdP): The party that manages the subscriber's primary authentication
346 credentials and issues Assertions derived from those credentials generally to the credential
347 service provider (CSP).
348

349 Identity Trust Framework: A Digital Identity System with established identity, security, privacy,
350 technology, and enforcement rules and policies adhered to by certified identity providers that
351 are members of the Identity Trust Framework. Members of an Identity Trust Framework
352 include Identity Trust Framework operators and identity providers. Relying Participants may be,
353 but are not required to be, a member of an Identity Trust Framework in order to accept an
354 identity credential issued by a certified identity provider to verify an identity credential holder's
355 identity. [§ 59.1-550, COV]
356

⁵ Federal Information Processing Standard (FIPS), accessible at <http://www.nist.gov/itl/fips.cfm>.

357 Information System: A discrete set of information resources organized for the collection,
358 processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST
359 Interagency/Internal Report (IR) 7298 r. 2]
360

361 Kerberos: A widely used authentication protocol developed at MIT. In “classic” Kerberos, users
362 share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to
363 communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by
364 the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords,
365 the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who
366 capture the initial user-to- KDC exchange. Longer password length and complexity provide
367 some mitigation to this vulnerability, although sufficiently long passwords tend to be
368 cumbersome for users.
369

370 Knowledge Based Authentication: Authentication of an individual based on knowledge of
371 information associated with his or her claimed identity in public databases. Knowledge of such
372 information is considered to be private rather than secret, because it may be used in contexts
373 other than authentication to a verifier, thereby reducing the overall assurance associated with
374 the authentication process.
375

376 Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the
377 attacker positions himself or herself in between the claimant and verifier so that he can
378 intercept and alter data traveling between them.
379

380 Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric
381 key to detect both accidental and intentional modifications of the data. MACs provide
382 authenticity and integrity protection, but not non-repudiation protection.
383

384 Multi-Factor: A characteristic of an authentication system or an authenticator that uses more
385 than one authentication factor. The three types of authentication factors are something you
386 know, something you have, and something you are.
387

388 Network: An open communications medium, typically the Internet, that is used to transport
389 messages between the claimant and other Participants. Unless otherwise stated, no
390 assumptions are made about the security of the network; it is assumed to be open and subject
391 to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e.,
392 eavesdropping) attack at any point between the Participants (e.g., claimant, verifier, CSP or RP).
393

394 Nonce: A value used in security protocols that is never repeated with the same key. For
395 example, nonces used as challenges in challenge-response authentication protocols must not
396 be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay
397 attack. Using a nonce as a challenge is a different requirement than a random challenge,
398 because a nonce is not necessarily unpredictable.
399

400 Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on
401 an authentication protocol run or by penetrating a system and stealing security files) that
402 he/she is able to analyze in a system of his/her own choosing.

404 Online Attack: An attack against an authentication protocol where the attacker either assumes
405 the role of a claimant with a genuine verifier or actively alters the authentication channel.

407 Online Guessing Attack: An attack in which an attacker performs repeated logon trials by
408 guessing possible values of the authenticator output.

410 Operational Authority: Entity responsible for operations, maintenance, management, and
411 related functions of an Identity Trust Framework.

413 Participant Requirements: A set of rules and policies in an Identity Trust Framework addressing
414 identity, security, privacy, technology, and enforcement, which are assigned to each member
415 type in a Digital Identity System. Member types include Registration Authorities (RAs), Identity
416 Providers (IdPs), Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs).
417 [§ 59.1-550, COV]

419 Passive Attack: An attack against an authentication protocol where the attacker intercepts data
420 traveling along the network between the claimant and verifier, but does not alter the data (i.e.,
421 eavesdropping).

423 Password: A secret that a claimant memorizes and uses to authenticate his or her identity.
424 Passwords are typically character strings.

426 Personal Identification Number (PIN): A password consisting only of decimal digits.

428 Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,
429 identity card, smart card) issued to federal employees and contractors that contains stored
430 credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that
431 the claimed identity of the cardholder can be verified against the stored credentials by another
432 person (human readable and verifiable) or an automated process (computer readable and
433 verifiable).

435 Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally
436 Identifiable Information means information that can be used to distinguish or trace an
437 individual's identity, either alone or when combined with other information that is linked or
438 linkable to a specific individual.

440 Pharming: An attack in which an attacker corrupts an infrastructure service such as DNS
441 (Domain Name Service) causing the Subscriber to be misdirected to a forged verifier/RP, which
442 could cause the Subscriber to reveal sensitive information, download harmful software or
443 contribute to a fraudulent act.

444 [Phishing: An attack in which the Subscriber is lured \(usually through an email\) to interact with a](#)
445 [counterfeit verifier/RP and tricked into revealing information that can be used to masquerade](#)
446 [as that Subscriber to the real verifier/RP.](#)

448 [Physical In-Person: Method of Identity Proofing in which Applicants are required to physically](#)
449 [present themselves and identity evidence to a representative of the Registration Authority or](#)
450 [Identity Trust Framework. \[NIST SP 800-63-2\]](#)

452 [Possession and control of an authenticator: The ability to activate and use the authenticator in](#)
453 [an authentication protocol.](#)

455 [Practice Statement: A formal statement of the practices followed by the Participants to an](#)
456 [authentication process \(i.e., RA, CSP, or verifier\). It usually describes the policies and practices](#)
457 [of the Participants and can become legally binding.](#)

459 [Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can](#)
460 [be used to compromise the authenticator.](#)

462 [Private Key: The secret part of an asymmetric key pair that is used to digitally sign or decrypt](#)
463 [data.](#)

465 [Protected Session: A session wherein messages between two participants are encrypted and](#)
466 [integrity is protected using a set of shared secrets called session keys. A participant is said to be](#)
467 [authenticated if, during the session, he, she or it proves possession of a long term authenticator](#)
468 [in addition to the session keys, and if the other Participant can verify the identity associated](#)
469 [with that authenticator. If both participants are authenticated, the protected session is said to](#)
470 [be mutually authenticated.](#)

472 [Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to](#)
473 [infer the Subscriber but which does permit the RP to associate multiple interactions with the](#)
474 [Subscriber's claimed identity.](#)

476 [Public Credentials: Credentials that describe the binding in a way that does not compromise the](#)
477 [authenticator.](#)

479 [Public Key: The public part of an asymmetric key pair that is used to verify signatures or encrypt](#)
480 [data.](#)

482 [Public Key Certificate: A digital document issued and digitally signed by the private key of a](#)
483 [Certificate authority that binds the name of a Subscriber to a public key. The certificate](#)
484 [indicates that the Subscriber identified in the certificate has sole control and access to the](#)
485 [private key. See also \[RFC 5280\].](#)

486

487 [Public Key Infrastructure \(PKI\): A set of policies, processes, server platforms, software and](#)
488 [workstations used for the purpose of administering certificates and public-private key pairs,](#)
489 [including the ability to issue, maintain, and revoke public key certificates.](#)
490
491 [Registration: The process through which an applicant applies to become a Subscriber of a CSP](#)
492 [and an RA validates the identity of the applicant on behalf of the CSP.](#)
493
494 [Registration Authority \(RA\): A trusted entity that establishes and vouches for the identity or](#)
495 [attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be](#)
496 [independent of a CSP, but it has a relationship to the CSP\(s\).](#)
497
498 [Relying Party \(RP\): An entity that relies upon the Subscriber's authenticator\(s\) and credentials](#)
499 [or a verifier's Assertion of a claimant's identity, typically to process a transaction or grant access](#)
500 [to information or a system.](#)
501
502 [Remote: \(As in remote authentication or remote transaction\) An information exchange](#)
503 [between network-connected devices where the information cannot be reliably protected end-](#)
504 [to-end by a single organization's security controls. Note: Any information exchange across the](#)
505 [Internet is considered remote.](#)
506
507 [Replay Attack: An attack in which the attacker is able to replay previously captured messages](#)
508 [\(between a legitimate claimant and a verifier\) to masquerade as that claimant to the verifier or](#)
509 [vice versa.](#)
510
511 [Risk Assessment: The process of identifying the risks to system security and determining the](#)
512 [probability of occurrence, the resulting impact, and additional safeguards that would mitigate](#)
513 [this impact. Part of Risk Management and synonymous with Risk Analysis.](#)
514
515 [Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the](#)
516 [results of computations for one instance cannot be reused by an attacker.](#)
517
518 [Secondary Authenticator: A temporary secret, issued by the verifier to a successfully](#)
519 [authenticated Subscriber as part of an Assertion protocol. This secret is subsequently used, by](#)
520 [the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer](#)
521 [Assertions, Assertion references, and Kerberos session keys.](#)
522
523 [Secure Sockets Layer \(SSL\): An authentication and security protocol widely implemented in](#)
524 [browsers and web servers. SSL has been superseded by the newer Transport Layer Security](#)
525 [\(TLS\) protocol; TLS 1.0 is effectively SSL version 3.1.](#)
526
527 [Security Assertion Mark-up Language \(SAML\): An XML-based security specification developed](#)
528 [by the Organization for the Advancement of Structured Information Standards \(OASIS\) for](#)
529 [exchanging authentication \(and authorization\) information between trusted entities over the](#)
530 [Internet.](#)

531 [SAML Authentication Assertion: A SAML Assertion that conveys information from a verifier to](#)
532 [an RP about a successful act of authentication that took place between the verifier and a](#)
533 [Subscriber.](#)

534
535 [Session Hijack Attack: An attack in which the attacker is able to insert himself or herself](#)
536 [between a claimant and a verifier subsequent to a successful authentication exchange between](#)
537 [the latter two Participants. The attacker is able to pose as a Subscriber to the verifier or vice](#)
538 [versa to control session data exchange. Sessions between the claimant and the relying](#)
539 [Participant can also be similarly compromised.](#)

540
541 [Shared Secret: A secret used in authentication that is known to the claimant and the verifier.](#)

542
543 [Social Engineering: The act of deceiving an individual into revealing sensitive information by](#)
544 [associating with the individual to gain confidence and trust.](#)

545
546 [Special Publication \(SP\): A type of publication issued by NIST. Specifically, the Special](#)
547 [Publication 800-series reports on the Information Technology Laboratory's research, guidelines,](#)
548 [and outreach efforts in computer security, and its collaborative activities with industry,](#)
549 [government, and academic organizations.](#)

550
551 [Strongly Bound Credentials: Credentials that describe the binding between a user and](#)
552 [authenticator in a tamper-evident fashion.](#)

553
554 [Subscriber: A Participant who has received a credential or authenticator from a CSP.](#)

555
556 [Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation](#)
557 [and its inverse, for example to encrypt and decrypt, or create a message authentication code](#)
558 [and to verify the code.](#)

559
560 [Token: See Authenticator.](#)

561
562 [Token Authenticator: See Authenticator Output.](#)

563
564 [Token Secret: See Authenticator Secret.](#)

565
566 [Transport Layer Security \(TLS\): An authentication and security protocol widely implemented in](#)
567 [browsers and web servers. TLS is defined by \[RFC 5246\]. TLS is similar to the older Secure](#)
568 [Sockets Layer \(SSL\) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52,](#)
569 [Guidelines for the Selection and Use of Transport Layer Security \(TLS\) Implementations specifies](#)
570 [how TLS is to be used in government applications.](#)

571
572 [Trust Anchor: A public or symmetric key that is trusted because it is directly built into hardware](#)
573 [or software, or securely provisioned via out-of-band means, rather than because it is vouched](#)
574 [for by another trusted entity \(e.g. in a public key certificate\).](#)

575 Unverified Name: A Subscriber name that is not verified as meaningful by Identity Proofing.

576

577 Valid: In reference to an ID, the quality of not being expired or revoked.

578

579 Verified Name: A Subscriber name that has been verified by Identity Proofing.

580

581 Verifier: An entity that verifies the claimant’s identity by verifying the claimant’s possession and

582 control of one or two authenticators using an authentication protocol. To do this, the verifier

583 may also need to validate credentials that link the authenticator(s) and identity and check their

584 status.

585

586 Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an

587 authentication protocol, usually to capture information that can be used to masquerade as a

588 claimant to the real verifier.

589

590 Virtual In-Person Proofing: A remote identity person proofing process that employs technical

591 and procedural measures that provide sufficient confidence that the remote session can be

592 considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]

593

594 Weakly Bound Credentials: Credentials that describe the binding between a user and

595 authenticator in a manner than can be modified without invalidating the credential.

596

597 Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero

598 so that the data is destroyed and not recoverable. This is often contrasted with deletion

599 methods that merely destroy reference to data within a file system rather than the data itself.

600

601 Zero-knowledge Password Protocol: A password based authentication protocol that allows a

602 claimant to authenticate to a Verifier without revealing the password to the verifier. Examples

603 of such protocols are EKE, SPEKE and SRP. Terms used in this document comply with definitions

604 in the Public Review version of the National Institute of Standards and Technology Special

605 Publication 800-63-3 (NIST SP 800-63-3), and align with adopted definitions in § 59.1-550, *Code*

606 *of Virginia*, and the Commonwealth of Virginia’s ITRM Glossary (ITRM Glossary).⁶

607

608 Active Attack: An online attack where the attacker transmits data to the claimant, credential

609 service provider, verifier, or relying party. Examples of active attacks include man-in-the-

610 middle, impersonation, and session hijacking.

611

⁶ NIST SP 800-63-3 may be accessed at <https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3. § 59.1-550, *Code of Virginia*, may be accessed at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/>. The Commonwealth’s ITRM Glossary may be accessed at http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV-ITRM-Glossary.pdf

612 Address of Record: The official location where an individual can be found. The address of record
613 always includes the residential street address of an individual and may also include the mailing
614 address of the individual. In very limited circumstances, an Army Post Office box number, Fleet
615 Post Office box number or the street address of next of kin or of another contact individual can
616 be used when a residential street address for the individual is not available.

617
618 Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An
619 algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2)
620 adopted in a FIPS or NIST Recommendation.

621
622 Applicant: A party undergoing the processes of registration and identity proofing.

623
624 Assertion: A statement from a verifier to a relying party (RP) that contains identity information
625 about a subscriber. Assertions may also contain verified attributes.

626
627 Assertion Reference: A data object, created in conjunction with an assertion, which identifies
628 the verifier and includes a pointer to the full assertion held by the verifier.

629
630 Assurance: In the context of [OMB M-04-04]⁷ and this document, assurance is defined as 1) the
631 degree of confidence in the vetting process used to establish the identity of an individual to
632 whom the credential was issued, and 2) the degree of confidence that the individual who uses
633 the credential is the individual to whom the credential was issued.

634
635 Asymmetric Keys: Two related keys, a public key and a private key that are used to perform
636 complementary operations, such as encryption and decryption or signature generation and
637 signature verification.

638
639 Attack: An attempt by an unauthorized individual to fool a verifier or a relying party into
640 believing that the unauthorized individual in question is the subscriber.

641
642 Attacker: A party who acts with malicious intent to compromise an information system.

643
644 Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or
645 something.

646
647 Authentication: The process of establishing confidence in the identity of users or information
648 systems.

649
650 Authentication Protocol: A defined sequence of messages between a claimant and a verifier
651 that demonstrates that the claimant has possession and control of a valid authenticator to

⁷ [OMB M-04-04] Office of Management and Budget, Memorandum 04-04: E-Authentication Guidance for Federal Agencies, accessible at <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>.

652 establish his/her identity, and optionally, demonstrates to the claimant that he or she is
653 communicating with the intended verifier.

654

655 Authentication Protocol Run: An exchange of messages between a claimant and a verifier that
656 results in authentication (or authentication failure) between the two parties.

657

658 Authentication Secret: A generic term for any secret value that could be used by an attacker to
659 impersonate the subscriber in an authentication protocol. These are further divided into short-
660 term authentication secrets, which are only useful to an attacker for a limited period of time,
661 and long term authentication secrets, which allow an attacker to impersonate the subscriber
662 until they are manually reset. The authenticator secret is the canonical example of a long term
663 authentication secret, while the authenticator output, if it is different from the authenticator
664 secret, is usually a short term authentication secret.

665

666 Authenticator: Something that the claimant possesses and controls (typically a cryptographic
667 module or password) that is used to authenticate the claimant's identity. In previous versions of
668 this guideline, this was referred to as a token.

669

670 Authenticator Assurance Level (AAL): A metric describing robustness of the authentication
671 process proving that the claimant is in control of a given subscriber's authenticator(s).

672

673 Authenticator Output: The output value generated by an authenticator. The ability to generate
674 valid authenticator outputs on demand proves that the claimant possesses and controls the
675 authenticator. Protocol messages sent to the verifier are dependent upon the authenticator
676 output, but they may or may not explicitly contain it.

677

678 Authenticator Secret: The secret value contained within an authenticator.

679 Authenticity: The property that data originated from its purported source.

680

681 Bearer Assertion: An assertion that does not provide a mechanism for the subscriber to prove
682 that he or she is the rightful owner of the assertion. The RP has to assume that the assertion
683 was issued to the subscriber who presents the assertion or the corresponding assertion
684 reference to the RP.

685

686 Bit: A binary digit: 0 or 1.

687

688 Biometrics: Automated recognition of individuals based on their behavioral and biological
689 characteristics. In this document, biometrics may be used to unlock authenticators and prevent
690 repudiation of registration.

691

692 Certificate Authority (CA): A trusted entity that issues and revokes public key certificates.

693

694 ~~Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally~~
695 ~~signed by a Certificate Authority. [RFC 5280]⁸~~
696
697 ~~Challenge Response Protocol: An authentication protocol where the verifier sends the claimant~~
698 ~~a challenge (usually a random value or a nonce) that the claimant combines with a secret (such~~
699 ~~as by hashing the challenge and a shared secret together, or by applying a private key operation~~
700 ~~to the challenge) to generate a response that is sent to the verifier. The verifier can~~
701 ~~independently verify the response generated by the claimant (such as by re-computing the hash~~
702 ~~of the challenge and the shared secret and comparing to the response, or performing a public~~
703 ~~key operation on the response) and establish that the claimant possesses and controls the~~
704 ~~secret.~~
705
706 ~~Claimant: A party whose identity is to be verified using an authentication protocol.~~
707
708 ~~Claimed Address: The physical location asserted by an individual (e.g. an applicant) where~~
709 ~~he/she can be reached. It includes the residential street address of an individual and may also~~
710 ~~include the mailing address of the individual. For example, a person with a foreign passport,~~
711 ~~living in the U.S., will need to give an address when going through the identity proofing process.~~
712 ~~This address would not be an “address of record” but a “claimed address.”~~
713
714 ~~Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth~~
715 ~~and address. [GPG45]⁹~~
716 ~~Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA): An~~
717 ~~interactive feature added to web forms to distinguish use of the form by humans as opposed to~~
718 ~~automated agents. Typically, it requires entering text corresponding to a distorted image or~~
719 ~~from a sound stream.~~
720
721 ~~Cookie: A character string, placed in a web browser’s memory, which is available to websites~~
722 ~~within the same Internet domain as the server that placed them in the web browser.~~
723
724 ~~Credential: An object or data structure that authoritatively binds an identity (and optionally,~~
725 ~~additional attributes) to an authenticator possessed and controlled by a subscriber. While~~
726 ~~common usage often assumes that the credential is maintained by the subscriber, this~~
727 ~~document also uses the term to refer to electronic records maintained by the CSP which~~
728 ~~establish a binding between the subscriber’s authenticator(s) and identity.~~
729

⁸ [RFC 5280] Official Internet Protocol Standards, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, accessible at <http://www.rfc-editor.org/info/rfc5280>.

⁹ [GPG 45] UK Cabinet Office, Good Practice Guide 45, Identity proofing and verification of an individual, November 3, 2014, accessible at <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>.

730 Credential Service Provider (CSP): A trusted entity that issues or registers subscriber
731 authenticators and issues electronic credentials to subscribers. The CSP may encompass
732 Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third
733 party, or may issue credentials for its own use.

734
735 Cross-Site Request Forgery (CSRF): An attack in which a subscriber who is currently
736 authenticated to an RP and connected through a secure session, browses to an attacker's
737 website which causes the subscriber to unknowingly invoke unwanted actions at the RP. For
738 example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to
739 unintentionally authorize a large money transfer, merely by viewing a malicious link in a
740 webmail message while a connection to the bank is open in another browser window.

741
742 Cross-Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an
743 otherwise benign website. These scripts acquire the permissions of scripts generated by the
744 target website and can therefore compromise the confidentiality and integrity of data transfers
745 between the website and client. Websites are vulnerable if they display user-supplied data from
746 requests or forms without sanitizing the data so that it is not executable.

747
748 Cryptographic Key: A value used to control cryptographic operations, such as decryption,
749 encryption, signature generation or signature verification. For the purposes of this document,
750 key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57
751 Part 1. See also Asymmetric keys, Symmetric key.

752
753 Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.

754
755 Data Integrity: The property that data has not been altered by an unauthorized entity.

756
757 Derived Credential: A credential issued based on proof of possession and control of an
758 authenticator associated with a previously issued credential, so as not to duplicate the identity
759 proofing process.

760 Digital Signature: An asymmetric key operation where the private key is used to digitally sign
761 data and the public key is used to verify the signature. Digital signatures provide authenticity
762 protection, integrity protection, and non-repudiation.

763
764 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication
765 protocol to capture information which can be used in a subsequent active attack to
766 masquerade as the claimant.

767
768 Electronic Authentication: The process of establishing confidence in user identities
769 electronically presented to an information system.

770
771 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value
772 of a secret. Entropy is usually stated in bits.

773

774 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes
775 a class of data objects called XML documents and partially describes the behavior of computer
776 programs which process them.
777

778 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal
779 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI
780 Policy Authority to create, sign, and issue public key certificates to Principal CAs.
781

782 Federal Information Security Management Act (FISMA): Title III of the E-Government Act
783 requiring each federal agency to develop, document, and implement an agency-wide program
784 to provide information security for the information and information systems that support the
785 operations and assets of the agency, including those provided or managed by another agency,
786 contractor, or other source.
787

788 Federal Information Processing Standard (FIPS): Under the Information Technology
789 Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards
790 and guidelines that are developed by the National Institute of Standards and Technology (NIST)
791 for Federal computer systems. These standards and guidelines are issued by NIST as Federal
792 Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when
793 there are compelling Federal government requirements such as for security and interoperability
794 and there are no acceptable industry standards or solutions.⁴⁰
795

796 Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string.
797 Approved hash functions satisfy the following properties:

- 798 • (One-way) It is computationally infeasible to find any input that maps to any pre-
799 specified output, and
- 800 • (Collision resistant) It is computationally infeasible to find any two distinct inputs that
801 map to the same output.

802 Holder-of-Key Assertion: An assertion that contains a reference to a symmetric key or a public
803 key (corresponding to a private key) held by the subscriber. The RP may authenticate the
804 subscriber by verifying that he or she can indeed prove possession and control of the
805 referenced key.
806

807 Identity: A set of attributes that uniquely describe a person within a given context.
808

809 Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's
810 claimed identity is their real identity.
811

812 Identity Proofing: The process by which a CSP and a Registration Authority (RA) collect and
813 verify information about a person for the purpose of issuing credentials to that person.
814

⁴⁰ Federal Information Processing Standard (FIPS), accessible at <http://www.nist.gov/itl/fips.cfm>.

815 Kerberos: A widely used authentication protocol developed at MIT. In “classic” Kerberos, users
816 share a secret password with a Key-Distribution-Center (KDC). The user, Alice, who wishes to
817 communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by
818 the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords,
819 the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who
820 capture the initial user-to-KDC exchange. Longer password length and complexity provide
821 some mitigation to this vulnerability, although sufficiently long passwords tend to be
822 cumbersome for users.

823
824 Knowledge-Based Authentication: Authentication of an individual based on knowledge of
825 information associated with his or her claimed identity in public databases. Knowledge of such
826 information is considered to be private rather than secret, because it may be used in contexts
827 other than authentication to a verifier, thereby reducing the overall assurance associated with
828 the authentication process.

829
830 Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the
831 attacker positions himself or herself in between the claimant and verifier so that he can
832 intercept and alter data traveling between them.

833
834 Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric
835 key to detect both accidental and intentional modifications of the data. MACs provide
836 authenticity and integrity protection, but not non-repudiation protection.

837
838 Multi-Factor: A characteristic of an authentication system or an authenticator that uses more
839 than one authentication factor. The three types of authentication factors are something you
840 know, something you have, and something you are.

841
842

843 **Network:** An open communications medium, typically the Internet, that is used to transport
844 messages between the claimant and other parties. Unless otherwise stated, no assumptions are
845 made about the security of the network; it is assumed to be open and subject to active (i.e.,
846 impersonation, man in the middle, session hijacking) and passive (i.e., eavesdropping) attack at
847 any point between the parties (e.g., claimant, verifier, CSP or RP).
848

849 **Nonce:** A value used in security protocols that is never repeated with the same key. For
850 example, nonces used as challenges in challenge-response authentication protocols must not
851 be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay
852 attack. Using a nonce as a challenge is a different requirement than a random challenge,
853 because a nonce is not necessarily unpredictable.
854

855 **Off-line Attack:** An attack where the attacker obtains some data (typically by eavesdropping on
856 an authentication protocol run or by penetrating a system and stealing security files) that
857 he/she is able to analyze in a system of his/her own choosing.
858

859 **Online Attack:** An attack against an authentication protocol where the attacker either assumes
860 the role of a claimant with a genuine verifier or actively alters the authentication channel.
861

862 **Online Guessing Attack:** An attack in which an attacker performs repeated logon trials by
863 guessing possible values of the authenticator output.
864

865 **Passive Attack:** An attack against an authentication protocol where the attacker intercepts data
866 traveling along the network between the claimant and verifier, but does not alter the data (i.e.,
867 eavesdropping).
868

869 **Password:** A secret that a claimant memorizes and uses to authenticate his or her identity.
870 Passwords are typically character strings.
871

872 **Personal Identification Number (PIN):** A password consisting only of decimal digits.
873

874 **Personal Identity Verification (PIV) Card:** Defined by [FIPS 201] as a physical artifact (e.g.,
875 identity card, smart card) issued to federal employees and contractors that contains stored
876 credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that
877 the claimed identity of the cardholder can be verified against the stored credentials by another
878 person (human readable and verifiable) or an automated process (computer readable and
879 verifiable).
880

881 **Personally Identifiable Information (PII):** As defined by OMB Circular A-130, Personally
882 Identifiable Information means information that can be used to distinguish or trace an
883 individual's identity, either alone or when combined with other information that is linked or
884 linkable to a specific individual.
885

886 ~~Pharming: An attack in which an attacker corrupts an infrastructure service such as DNS~~
887 ~~(Domain Name Service) causing the subscriber to be misdirected to a forged verifier/RP, which~~
888 ~~could cause the subscriber to reveal sensitive information, download harmful software or~~
889 ~~contribute to a fraudulent act.~~

890

891 ~~Phishing: An attack in which the subscriber is lured (usually through an email) to interact with a~~
892 ~~counterfeit verifier/RP and tricked into revealing information that can be used to masquerade~~
893 ~~as that subscriber to the real verifier/RP.~~

894

895 ~~Possession and control of an authenticator: The ability to activate and use the authenticator in~~
896 ~~an authentication protocol.~~

897

898 ~~Practice Statement: A formal statement of the practices followed by the parties to an~~
899 ~~authentication process (i.e., RA, CSP, or verifier). It usually describes the policies and practices~~
900 ~~of the parties and can become legally binding.~~

901

902 ~~Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can~~
903 ~~be used to compromise the authenticator.~~

904

905 ~~Private Key: The secret part of an asymmetric key pair that is used to digitally sign or decrypt~~
906 ~~data.~~

907

908 ~~Protected Session: A session wherein messages between two participants are encrypted and~~
909 ~~integrity is protected using a set of shared secrets called session keys. A participant is said to be~~
910 ~~authenticated if, during the session, he, she or it proves possession of a long term authenticator~~
911 ~~in addition to the session keys, and if the other party can verify the identity associated with that~~
912 ~~authenticator. If both participants are authenticated, the protected session is said to be~~
913 ~~mutually authenticated.~~

914

915 ~~Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to~~
916 ~~infer the subscriber but which does permit the RP to associate multiple interactions with the~~
917 ~~subscriber's claimed identity.~~

918

919 ~~Public Credentials: Credentials that describe the binding in a way that does not compromise the~~
920 ~~authenticator.~~

921

922 ~~Public Key: The public part of an asymmetric key pair that is used to verify signatures or encrypt~~
923 ~~data.~~

924

925 ~~Public Key Certificate: A digital document issued and digitally signed by the private key of a~~
926 ~~Certificate authority that binds the name of a subscriber to a public key. The certificate~~
927 ~~indicates that the subscriber identified in the certificate has sole control and access to the~~
928 ~~private key. See also [RFC 5280].~~

929

930 ~~Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and~~
931 ~~workstations used for the purpose of administering certificates and public-private key pairs,~~
932 ~~including the ability to issue, maintain, and revoke public key certificates.~~
933
934 ~~Registration: The process through which an applicant applies to become a subscriber of a CSP~~
935 ~~and an RA validates the identity of the applicant on behalf of the CSP.~~
936
937 ~~Registration Authority (RA): A trusted entity that establishes and vouches for the identity or~~
938 ~~attributes of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be~~
939 ~~independent of a CSP, but it has a relationship to the CSP(s).~~
940
941 ~~Relying Party (RP): An entity that relies upon the subscriber's authenticator(s) and credentials~~
942 ~~or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access~~
943 ~~to information or a system.~~
944
945 ~~Remote: (As in remote authentication or remote transaction) An information exchange~~
946 ~~between network-connected devices where the information cannot be reliably protected end-~~
947 ~~to-end by a single organization's security controls. Note: Any information exchange across the~~
948 ~~Internet is considered remote.~~
949
950 ~~Replay Attack: An attack in which the attacker is able to replay previously captured messages~~
951 ~~(between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or~~
952 ~~vice-versa.~~
953
954 ~~Risk Assessment: The process of identifying the risks to system security and determining the~~
955 ~~probability of occurrence, the resulting impact, and additional safeguards that would mitigate~~
956 ~~this impact. Part of Risk Management and synonymous with Risk Analysis.~~
957
958 ~~Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the~~
959 ~~results of computations for one instance cannot be reused by an attacker.~~
960
961 ~~Secondary Authenticator: A temporary secret, issued by the verifier to a successfully~~
962 ~~authenticated subscriber as part of an assertion protocol. This secret is subsequently used, by~~
963 ~~the subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer~~
964 ~~assertions, assertion references, and Kerberos session keys.~~
965
966 ~~Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in~~
967 ~~browsers and web servers. SSL has been superseded by the newer Transport Layer Security~~
968 ~~(TLS) protocol; TLS 1.0 is effectively SSL version 3.1.~~
969
970 ~~Security Assertion Mark up Language (SAML): An XML-based security specification developed~~
971 ~~by the Organization for the Advancement of Structured Information Standards (OASIS) for~~
972 ~~exchanging authentication (and authorization) information between trusted entities over the~~
973 ~~Internet.~~

974 SAML Authentication Assertion: A SAML assertion that conveys information from a verifier to
975 an RP about a successful act of authentication that took place between the verifier and a
976 subscriber.
977

978 Session Hijack Attack: An attack in which the attacker is able to insert himself or herself
979 between a claimant and a verifier subsequent to a successful authentication exchange between
980 the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to
981 control session data exchange. Sessions between the claimant and the relying party can also be
982 similarly compromised.
983

984 Shared Secret: A secret used in authentication that is known to the claimant and the verifier.
985

986 Social Engineering: The act of deceiving an individual into revealing sensitive information by
987 associating with the individual to gain confidence and trust.
988

989 Special Publication (SP): A type of publication issued by NIST. Specifically, the Special
990 Publication 800-series reports on the Information Technology Laboratory's research, guidelines,
991 and outreach efforts in computer security, and its collaborative activities with industry,
992 government, and academic organizations.
993

994 Strongly Bound Credentials: Credentials that describe the binding between a user and
995 authenticator in a tamper-evident fashion.
996

997 Subscriber: A party who has received a credential or authenticator from a CSP.
998

999 Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation
1000 and its inverse, for example to encrypt and decrypt, or create a message authentication code
1001 and to verify the code.
1002

1003 Token: See Authenticator.
1004

1005 Token Authenticator: See Authenticator Output.
1006

1007 Token Secret: See Authenticator Secret.
1008

1009 Transport Layer Security (TLS): An authentication and security protocol widely implemented in
1010 browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure
1011 Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52,
1012 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies
1013 how TLS is to be used in government applications.
1014

1015 Trust Anchor: A public or symmetric key that is trusted because it is directly built into hardware
1016 or software, or securely provisioned via out-of-band means, rather than because it is vouched
1017 for by another trusted entity (e.g. in a public key certificate).

1018 ~~Trust Framework: In identity management, means a digital identity system with established~~
1019 ~~identity, security, privacy, technology, and enforcement rules and policies adhered to by~~
1020 ~~certified identity providers that are members of the identity trust framework. Members of an~~
1021 ~~identity trust framework include identity trust framework operators and identity providers.~~
1022 ~~Relying parties may be, but are not required to be, a member of an identity trust framework in~~
1023 ~~order to accept an identity credential issued by a certified identity provider to verify an identity~~
1024 ~~credential holder's identity. [§ 59.1-550, Code of Virginia]~~
1025
1026 ~~Unverified Name: A subscriber name that is not verified as meaningful by identity proofing.~~
1027
1028 ~~Valid: In reference to an ID, the quality of not being expired or revoked.~~
1029
1030 ~~Verified Name: A subscriber name that has been verified by identity proofing.~~
1031
1032 ~~Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and~~
1033 ~~control of one or two authenticators using an authentication protocol. To do this, the verifier~~
1034 ~~may also need to validate credentials that link the authenticator(s) and identity and check their~~
1035 ~~status.~~
1036
1037 ~~Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an~~
1038 ~~authentication protocol, usually to capture information that can be used to masquerade as a~~
1039 ~~claimant to the real verifier.~~
1040
1041 ~~Weakly Bound Credentials: Credentials that describe the binding between a user and~~
1042 ~~authenticator in a manner that can be modified without invalidating the credential.~~
1043
1044 ~~Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero~~
1045 ~~so that the data is destroyed and not recoverable. This is often contrasted with deletion~~
1046 ~~methods that merely destroy reference to data within a file system rather than the data itself.~~
1047
1048 ~~Zero-knowledge Password Protocol: A password-based authentication protocol that allows a~~
1049 ~~claimant to authenticate to a Verifier without revealing the password to the verifier. Examples~~
1050 ~~of such protocols are EKE, SPEKE and SRP.~~

1051 **56 Background**

1052 In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter
1053 [50 of Title 59.1, Code of Virginia](#)) to address demand in the state’s digital economy for secure,
1054 privacy enhancing ~~electronic authentication~~ [Electronic Authentication](#) and identity
1055 management. Growing numbers of “communities of interest” have advocated for stronger,
1056 scalable and interoperable identity solutions to increase consumer protection and reduce
1057 liability for principal actors in the identity ecosystem – Identity Providers, Credential Service
1058 Providers and Relying Parties.

1061 [To address the demand contemplated by the Electronic Identity Management Act, the General
1062 Assembly also created the Identity Management Standards Advisory Council \(IMSAC\) to advise
1063 the Secretary of Technology on the adoption of identity management standards and the
1064 creation of guidance documents, pursuant to §2.2-436. A copy of the IMSAC Charter has been
1065 provided in \[Appendix 1\]\(#\). The following guidance document has been developed by the Virginia
1066 Information Technologies Agency \(VITA\), acting on behalf of the Secretary of Technology and
1067 Chief Information Officer of the Commonwealth, at the direction of IMSAC. IMSAC was created
1068 by the General Assembly as part of the Act and advises the Secretary of Technology on the
1069 adoption of identity management standards and the creation of guidance documents pursuant
1070 to §2.2-436. A copy of the IMSAC Charter has been provided in \[Appendix 1\]\(#\).](#)

1072 The Advisory Council recommends to the Secretary of Technology guidance documents relating
1073 to (i) nationally recognized technical and data standards regarding the verification and
1074 authentication of identity in digital and online transactions; (ii) the minimum specifications and
1075 standards that should be included in an ~~identity~~ [Identity](#) Trust Framework, as defined in §59.1-
1076 550, so as to warrant liability protection pursuant to the Electronic Identity Management Act
1077 (§59.1-550 et seq.); and (iii) any other related data standards or specifications concerning
1078 reliance by third ~~parties~~ [Participants](#) on identity credentials, as defined in §59.1-550.

1080 **Purpose Statement**

1081 [This guidance document, as defined in § 2.2-4001, was developed by the Identity Management
1082 Standards Advisory Council \(IMSAC\), on behalf of the Secretary of Technology, to provide
1083 information or guidance of general applicability to the public for interpreting or implementing
1084 the Electronic Identity Management Act. Specifically, the document establishes ~~The purpose of
1085 this document is to establish~~ minimum specifications for ~~electronic Federation and Participant
1086 Requirements authentication within an identity management system~~ a \[Digital Identity System\]\(#\).
1087 ~~The document assumes that the identity management system will be supported by a trust~~](#)

1089 ~~framework, compliant with Applicable Law.~~⁴⁴ The minimum specifications have been stated
 1090 ~~based on language in~~ designed to be conformant with NIST SP 800-63C-3.
 1091

1092 The document defines ~~governance models, minimum requirements, processes, assurance levels,~~
 1093 ~~and Participant Requirements for a Federated Digital Identity System, components, process~~
 1094 ~~flows, assurance levels and privacy and security provisions for electronic authentication.~~ The
 1095 document assumes that specific ~~business, legal and technical requirements for electronic~~
 1096 ~~authentication~~ Participant Requirements will be established in the ~~Trust Framework~~ Identity
 1097 ~~Trust Framework~~ for each distinct ~~identity management system~~ Digital Identity System, and that
 1098 these requirements will be designed based on the ~~Electronic Authentication model and~~
 1099 ~~Federation Identity Assurance Level (IA/FAL) requirements) and Authenticator Assurance Level~~
 1100 ~~(AAL) requirements~~ for the system.

1102 The document limits its focus to ~~electronic authentication~~ Federation and Participant
 1103 ~~Requirements.~~ Minimum specifications for other components ~~of an identity management~~
 1104 ~~system~~ a Digital Identity System ~~will behave been~~ defined in separate IMSAC guidance
 1105 documents in this series, pursuant to §2.2-436 and §2.2-437.
 1106

1107 **6.7 Minimum Specifications**

1108 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3)
 1109 defines ~~an “electronic authentication Federation” in a Digital Identity System~~ as “A process that
 1110 ~~allows for the conveyance of identity and authentication information across a set of networked~~
 1111 ~~systems~~ the process of establishing confidence in the identity of users or information
 1112 ~~systems.”¹² Information systems may use the authenticated identity to determine if that user is~~
 1113 ~~authorized to perform an electronic transaction. Federation of a Digital Identity System~~
 1114 ~~depends upon each member, or Participant, in the system complying with Participant~~
 1115 ~~Requirements, the set of rules and policies assigned to each member type by the system’s~~
 1116 ~~Identity Trust Framework.~~
 1117

1119 This document establishes minimum specifications for ~~electronic authentication~~ Federation and
 1120 ~~Participant Requirements in a Digital Identity System~~ conformant with ~~and using language~~
 1121 ~~from~~ NIST SP 800-63-3. However, the minimum specifications defined in this document have
 1122 been developed to accommodate requirements for ~~electronic authentication~~ Federation and

⁴⁴ ~~For the purpose of this guidance document, the term “Applicable Law” shall mean laws, statutes, regulations,~~
~~and rules of the jurisdiction in which each participant in an identity management system member of an Identity~~
~~Trust Framework operates.~~

¹² The Public Review version of National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) may be accessed at <https://pages.nist.gov/800-63-3/sp800-63-3.html>. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.

1123 ~~Participant Requirements~~ established under other national and international standards.¹³ ~~The~~
 1124 ~~minimum specifications in this document also assume that specific business, legal and technical~~
 1125 ~~requirements for an identity management system will be documented in the trust framework~~
 1126 ~~for that system.~~ Minimum specifications for other components of ~~an identity management~~
 1127 ~~system~~ a Digital Identity System have been documented in separate guidance documents in the
 1128 IMSAC series, pursuant to §2.2-436 and §2.2-437.

1129 Electronic Authentication Model

1130 Electronic ~~authentication~~ Authentication is the process of establishing confidence in
 1131 individual identities presented to a ~~digital system~~ Digital Identity System. In a Federated Digital
 1132 Identity Systems, Electronic Authentication and related flows of identity information occur
 1133 across a set of network systems. These systems are often run and controlled by disparate
 1134 members in different network and security domains can use the authenticated identity to
 1135 determine if that individual is authorized to perform an online transaction. The minimum
 1136 specifications in this document assume that the authentication and transaction take place
 1137 across a network. Therefore, Federation requires Electronic Authentication models to be
 1138 extended to take into account the roles played by each member type and the corresponding
 1139 Participant Requirements.

1140 ~~The electronic authentication model~~ The minimum specifications for Federation and Participant
 1141 Requirements defined in this document reflect the Electronic Authentication model defined in
 1142 these minimum specifications reflects current technologies and architectures used primarily by
 1143 governmental entities. More complex models that separate functions among a broader range
 1144 of ~~parties~~ Participants are also available and may have advantages in some classes of
 1145 applications. While a simpler model ~~has been defined in~~ serves as the basis for these minimum
 1146 specifications, it does not preclude ~~participant member~~ s in identity management system Digital
 1147 Identity Systems from separating these functions. Minimum specifications for the Electronic
 1148 Authentication model reflected in this document have been defined in IMSAC Guidance
 1149 Document: Electronic Authentication, and a graphic of the model has been shown in Figure 1.

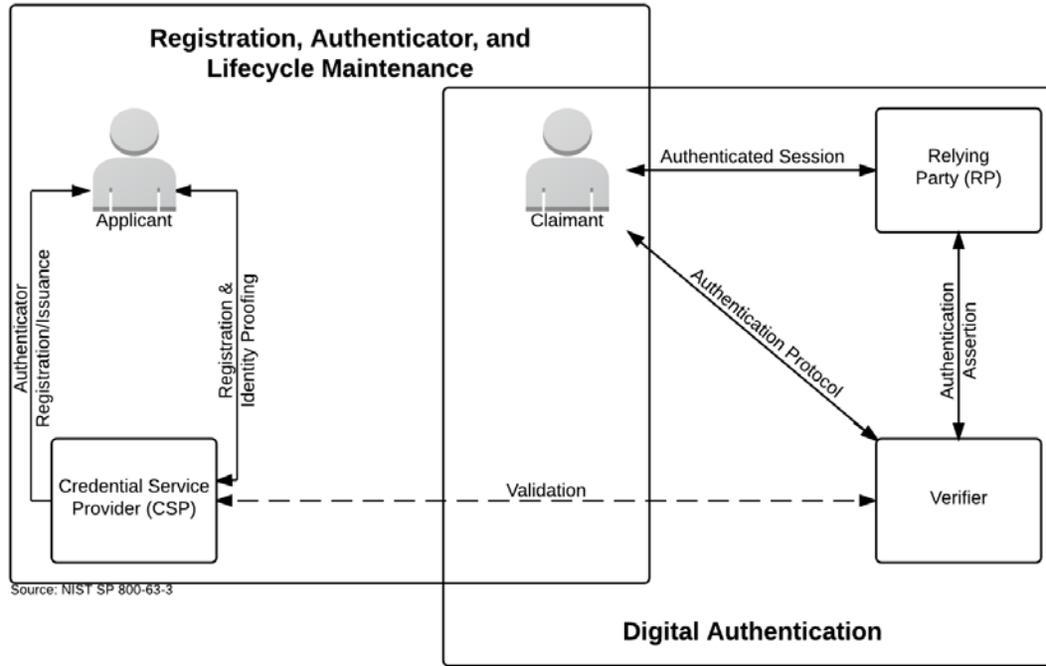
Formatted: Font: Italic

Formatted: Font: Bold

¹³ The minimum specifications defined in this document align with the State Identity Credential and Access Management (SICAM) Guidance and Roadmap, published by the National Association of State Chief Information Officers (NASCIO): <http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf>; and the Identity Ecosystem Framework (IDEF), published by the Identity Ecosystem Steering Group (IDESG): <https://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents>.

1153

Figure 1. Electronic Authentication Model



Formatted: Width: 11", Height: 8.5"
Formatted: Centered

1154

1155

1156

1157

1158

1159

1160

Source: NIST SP 800-63-3, accessible at <https://pages.nist.gov/800-63-3/sp800-63-3.html>

Note: Figure 1 illustrates the model for Electronic Authentication in a Digital Identity System, as documented in NIST SP 800-63-3 (Public Review), containing all components, requirements, and specifications recommended by IMSAC. However, the minimum specifications defined in this document have been developed to accommodate requirements for Assertions established under other national and international standards.

Formatted: Centered, Indent: Left: 1",
Position: Vertical: -0.05", Relative to:
Paragraph

1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171

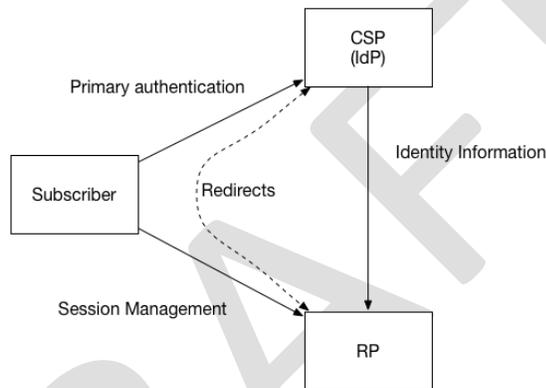
Federation

Federation is a process that allows for the conveyance of identity and authentication information across a set of networked systems. In a Federation scenario, the verifier or CSP is known as the identity provider, or IdP. In this document, the relying Participant, or RP, is the Participant that receives the Federated identity. **Figure 2** shows a common Federation model.

Formatted: Font: Bold

Figure 2: Federation Model

Formatted: Font: Bold



Formatted: Font: Bold

Formatted: Centered

Formatted: Font: Bold

1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190

In a Federation protocol, a triangle is formed between the Subscriber, the IdP, and the RP. Depending on the specifics of the protocol, different information passes across each leg of the triangle at different times. The Subscriber communicates with both the IdP and the RP, usually through a web browser. The RP and the IdP communicate with each other, though this communication can happen over the front channel (through redirects involving the Subscriber), over the back channel (through a direct connection), or via a packaged information bundle (such as a cryptographically protected and self-contained Assertions).

The Subscriber authenticates to the IdP using some form of primary credential, and then that authentication event is asserted to the RP across the network. The IdP can also make attribute statements about the Subscriber as part of this process. Attributes and authentication event information are usually carried to the RP through the use of an Assertion. Minimum specifications for Assertions have been documented in *IMSAC Guidance Document: Digital Identity Assertions*.

Formatted: Font: Italic

The RP communication with the IdP reveals to the IdP where the Subscriber is conducting a transaction. Communications from multiple RPs allow the IdP to build a profile of Subscriber transactions that would not have existed absent Federation. This aggregation could enable new

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1191 capabilities for Subscriber tracking and use of profile information that do not align with the
1192 privacy interests of the Subscribers.

1193
1194 The IdP must not disclose information on Subscriber activities at an RP to any Participant, nor
1195 use the information for any purpose other than Federated authentication, to comply with law
1196 or legal process, or in the case of a specific user request for the information. The IdP SHOULD
1197 employ technical measures to provide unlinkability and prevent Subscriber activity tracking and
1198 profiling. A IdP may disclose information on Subscriber activities to other RPs within the
1199 Federation for security purposes such as communication of compromised Subscriber accounts.

1200 1201 Federation Models

Formatted: Font: 13 pt

1202
1203 This section provides an overview of a few common models of identity Federation currently in
1204 use. In these models, a relationship is established between Participants of the Federation in
1205 several different ways. Some models mandate that all Federated Participants have an equally
1206 high level of trust, while other models allow for Participants with a diversity of relationships.

1207 1208 Central Authority

1209 Some Federated Participants defer to a central authority to make decisions for them and to
1210 communicate metadata between Participants. In this model, the central authority generally
1211 conducts some level of vetting on each Participant in the Federation to verify compliance with
1212 predetermined security and integrity standards.

1213
1214 Most Federations using the central authority model have a simple membership model - either
1215 Participants are in the Federation or they are not. However, more sophisticated Federations
1216 have multiple tiers of membership which can be used by Federated Participants to tell whether
1217 other Participants in the Federation have been more thoroughly vetted or have some common
1218 purpose that justifies a higher level of access. As a consequence, some Participants in the
1219 Federation are more likely to automatically release information about their Subscribers to the
1220 Participants in the higher tiers.

1221 1222 Manual Registration

1223 In the manual registration model of Federation, system administrators communicate metadata
1224 and test system interoperability before transactions take place between users over the wire.
1225 Metadata for each Participant who wishes to participate is manually input into a registry of
1226 Federated Participants. Each Participant maintains their own registry of other Participants with
1227 whom they wish to federate.

1228
1229 Manual registration can take place on a case by case basis without any authority or Federation
1230 operator in place. In this case, a pairwise relationship is created between the IdP and the RP.

1231
1232 Manual registration can also work in concert with a central authority model. In this case, a
1233 registry is pre-populated with Participants known to the central authority, and more
1234 Participants are added manually on an as-needed basis.

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274

Dynamic Registration

In the dynamic registration model of Federation, systems have a well-known location where other systems can find their metadata. They also have predictable API endpoints where new systems can register themselves without human involvement. Systems that make use of dynamic registration SHOULD require verifiable human interaction, such as the approval of the identity Federation transaction by the authenticated Subscriber at the IdP.

Each Federated Participant sets attribute and information access policies for other Federated Participants. In a dynamic registration environment, a newly registered Participant could be severely limited in its access until such time as it is reviewed by an authorized Participant. For instance, a system administrator can grant higher levels of access. Additionally, a dynamically registered Participant will usually also require authorization from a Subscriber during the authentication transaction (see Runtime Decisions).

Frequently, Participants in a dynamic registration model have no way to know each other ahead of time. As a consequence, little information about users and systems is exchanged by default. This problem is somewhat mitigated by a technology called software statements, which allow Federated Participants to cryptographically verify some attributes of the Participants involved in dynamic registration. Software statements are lists of attributes describing the RP software, cryptographically signed by certifying bodies. Because both Participants trust the certifying body, that trust can be extended to the other Participant in the dynamic registration partnership. This allows the connection to be established or elevated between the federating Participants without relying on self-asserted attributes entirely.

Proxied Federation

In a proxied Federation model, the communication between the IdP and the RP is proxied in a way that prevents direct communication between the two Participants. There may be multiple methods of achieving this effect, but common configurations include a third Participant that acts as a Federation proxy (or “broker”) or a network of “nodes” that distribute the communications. **Figure 3** shows a Federation proxy model.

Effectively, the Participants still function in some degree as a Federation IdP on one side and a Federation RP on the other side. Notably, a Federation proxy acts as an IdP to all Federated RPs and as an RP to all Federated IdPs. Therefore, all normative requirements that apply to IdPs and RPs SHALL apply to the Participants of such a system in their respective roles.

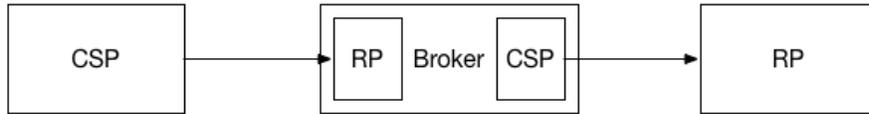
Formatted: Font: Bold

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1275

Figure 3: Federation Proxy Model

Formatted: Font: Bold



1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

A proxied Federation model can provide various benefits. For example, Federation proxies can enable simplified technical integrations between the RP and IdP by eliminating the need for multiple point to point integrations, which can be onerous for protocols which do not support dynamic registration. Additionally, to the extent a proxied Federation model effectively blinds the RP and IdP from each other, it can provide some business confidentiality for organizations that may not wish to reveal their Subscriber lists to each other, as well as mitigate some of the privacy risks of point to point Federation described above.

1286

1287

1288

1289

1290

1291

1292

1293

1294

While some proxied deployments offer no additional privacy protection (such as those that exist as integration points), others can offer varying levels of privacy to the Subscriber through a range of blinding technologies. It should be noted that even with the use of blinding technologies, it may still be possible for a blinded Participant to deduce Subscriber behavior patterns through analysis of timestamps, cookies, attributes, or attribute bundle sizes. Privacy policies may dictate appropriate use by the IdP, RP, and the Federation proxy, but blinding technology can increase effectiveness of these policies by making the data more difficult to access. It should also be noted that as the level of blinding increases, so does the technical and operational implementation complexity.

1295

1296

The following list documents a spectrum of blinding implementations:

1297

1298

1299

1300

1301

1302

1303

1304

1305

1306

1307

1308

1309

1310

1311

- The Federation proxy does not blind the RP and IdP from one another. The Federation proxy is able to monitor and track all Subscriber relationships between the RPs and IdPs, and has visibility into any attributes it is transmitting in the Assertions.
- The Federation proxy does not blind the RP and IdP from one another. The Federation proxy is able to monitor and track all Subscriber relationships between the RPs and IdPs, but has no visibility into any attributes it is transmitting in the Assertions.
- The Federation proxy blinds the RP and IdP from each other. The Federation proxy is able to monitor and track all Subscriber relationships between the RPs and IdPs, and has visibility into any attributes it is transmitting in the Assertions.
- The Federation proxy blinds the RP and IdP from each other. The Federation proxy is able to monitor and track all Subscriber relationships between the RPs and IdPs, but has no visibility into any attributes it is transmitting in the Assertions.
- The Federation proxy blinds the RP, IdP, and itself. The Federation proxy cannot monitor or track any Subscriber relationships, and has no visibility into any attributes it is transmitting in the Assertions.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354

Runtime Decisions

Formatted: Font: 13 pt

The fact that Federated Participants are known to each other through some form of registration or centralized management does not necessarily mean they are allowed to pass information. Federated Participants can establish whitelists of other Federated Participants who may authenticate Subscribers or pass information about them without runtime authorization from the Subscriber.

Federated Participants also can establish blacklists of other Federated Participants who may not be allowed to pass information about Subscribers at all. Every Participant that is not on a whitelist or a blacklist is placed by default in a gray area where runtime authorization decisions will be made by an authorized Participant, often the Subscriber.

Federation Assurance Level

Formatted: Font: 13 pt

This section defines allowable Federation Assurance Levels (FAL). The FAL describes aspects of the Assertion and Federation protocol used in a given transaction. These levels can be requested by an RP or required by configuration of both RP and IdP for a given transaction.

The FAL combines aspects of Assertion protection strength and Assertion presentation into a single, increasing scale applicable across different Federation models. While many other combinations of factors are possible, this list is intended to provide clear implementation guidelines representing increasingly secure deployment choices. Combinations of aspects not found in the FAL table are possible but outside the scope of this document.

Examples of Assertions Protocols:

- SAML Assertions – Security Assertion Markup Language (SAML) Assertions are specified using a mark-up language intended for describing security Assertions. They can be used by a verifier to make a statement to an RP about the identity of a claimant. SAML assertions may optionally be digitally signed.
- OpenID Connect Claims - OpenID Connect are specified using JavaScript Object Notation (JSON) for describing security, and optionally, user claims. JSON user info claims may optionally be digitally signed.
- Kerberos Tickets – Kerberos Tickets allow a ticket granting authority to issue session keys to two authenticated parties using based encapsulation schemes.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Table 1 presents different requirements depending on whether the Assertion is presented through either the front channel or the back channel (via an Assertion reference). Each successive level subsumes and fulfills all requirements of lower levels. Federations presented through a proxy must be represented by the lowest level used during the proxied transaction.

Formatted: Font: Bold

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1355
1356

Table 1. FAL Requirements by Back-Channel v. Front-Channel Assertions

FAL	Back-Channel Presentation Requirement	Front-Channel Presentation Requirement
<u>1</u>	<u>Bearer Assertion, asymmetrically signed by IdP</u>	<u>Bearer Assertion, asymmetrically signed by IdP</u>
<u>2</u>	<u>Bearer Assertion, asymmetrically signed by IdP</u>	<u>Bearer Assertion, asymmetrically signed by IdP and encrypted to RP</u>
<u>3</u>	<u>Bearer Assertion, asymmetrically signed by IdP and encrypted to RP</u>	<u>Bearer Assertion, asymmetrically signed by IdP and encrypted to RP</u>
<u>4</u>	<u>Holder of key Assertion, asymmetrically signed by IdP and encrypted to RP</u>	<u>Holder of key Assertion, asymmetrically signed by IdP and encrypted to RP</u>

- Formatted: Space After: 6 pt
- Formatted: Font: Bold
- Formatted: Font: 10.5 pt
- Formatted: Font: 10.5 pt
- Formatted: Centered
- Formatted Table
- Formatted: Font: 10.5 pt
- Formatted: Font: 10.5 pt
- Formatted: Centered

1357

For example, FAL 1 maps to the OpenID Connect Implicit Client profile or the SAML Web SSO profile, with no additional features. FAL 2 maps to the OpenID Connect Basic Client profile or the SAML Artifact Binding profile, with no additional features.

1358
1359
1360
1361
1362
1363
1364
1365
1366

FAL 3 additionally requires that the OpenID Connect ID Token or SAML Assertion be encrypted to a public key representing the RP in question. FAL 4 requires the presentation of an additional key bound to the Assertion (for example, the use of a cryptographic authenticator) along with all requirements of FAL3. Note that the additional key presented at FAL 4 need not be the same key used by the subscriber to authenticate to the IdP.

1367
1368
1369
1370
1371
1372

Regardless of what is requested or required by the protocol, the applicable FAL is easily detected by the RP by observing the nature of the Assertion as it is presented as part of the Federation protocol. Therefore, the RP is responsible for determining which FALS it is willing to accept for a given authentication transaction and ensuring that the transaction meets the requirements of that FAL.

1373

Participant Requirements

1374
1375
1376
1377
1378
1379
1380

The following section defines the minimum specifications for Participant Requirements in a Federated Digital Identity System. These minimum specifications build upon the trust agreements documented in the State Identity Credential and Access Management (SICAM) Guidance and Roadmap, published by the National Association of State Chief Information Officers (NASCIO).

1381

Participants include Registration Authorities (RAs), Identity Providers (IdPs), Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs). These minimum specifications assume that specific Participant Requirements will be established in the Identity Trust Framework for each Digital Identity System. For more information, see *IMSAC Guidance Document: Identity Trust Frameworks*.

1382
1383
1384
1385
1386
1387

Formatted: Font: Italic

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1388 Registration Authorities (RAs)
 1389 RAs establish and vouch for the Identity or Attributes of an Applicant to a CSP. RAs may be an
 1390 integral part of a CSP, or it may be independent of a CSP, but it maintains a trusted relationship
 1391 to the CSP(s). Primary requirements for RAs include the following:

- 1392 • Perform Physical or Virtual In-Person Proofing functions on identity evidence submitted
 1393 by an Applicant for a Claimed Identity
- 1394 • Verify and validate identity evidence submitted by an Applicant to support a Claimed
 1395 Identity during a Registration event.
- 1396 • Perform Registration (or enrollment) of Applicants for which the Claimed Identity has
 1397 been verified, validated, and accepted
- 1398 • Issue an appropriate Credential to a registered Subscriber who has completed the
 1399 Registration process
- 1400 • Manage, monitor, and audit the usage of Credentials by Subscribers who have
 1401 Registered with the RA
- 1402 • Establish and implement a process to revoke a Subscriber’s Credential in the event of
 1403 improper use, irregularities, or a security breach
- 1404 • Manage required post-issuance updates or modifications to a Subscriber’s Credential
 1405 based on verified and validated changes in the Claimed Identity or identity evidence
- 1406 • Establish and implement a process to re-issue a Subscriber’s Credential when corrective
 1407 action has been taken or the identity evidence has been updated

Formatted: List Paragraph, Bulleted + Level: 1
 + Aligned at: 0.25" + Indent at: 0.5"

1408 Identity Providers (IdPs)
 1409 IdPs manage the Subscriber’s primary authentication Credentials and issue Assertions derived
 1410 from those Credentials, generally to the CSP. Primary requirements for IdPs include the
 1411 following:

- 1413 • Provide a trust model that ensures that an individual is linked to identities which have
 1414 been issued, protected, and managed to provide the accuracy of asserted Attributes
- 1415 • Develop and provide an Authentication process by which the user (Subscriber or
 1416 Applicant) provides evidence to the IdP, who independently verifies that the user is who
 1417 he or she claims to be
- 1418 • Develop a process to periodically reevaluate the status of the user and the validity of his
 1419 or her associated Identity
- 1420 • Develop a process for Attribute management to ensure the timely cancellation or
 1421 modification of Attributes should the user’s status change
- 1422 • Develop a process for auditing the Attribute identification process, including registration
 1423 activities, to ensure Attributes are maintained in accordance with the process specified
 1424 by that IdP
- 1425 • Conduct audit functions in a manner to identify any irregularities or security breaches
- 1426 • Provide to the Federation audit information, upon request
- 1427 • Provide a process to assist users who have either lost or forgotten their means of
 1428 Authentication

Formatted: List Paragraph, Bulleted + Level: 1
 + Aligned at: 0.25" + Indent at: 0.5"

1429
 1430

Formatted: Position: Vertical: -0.04", Relative
 to: Paragraph

1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462

Credential Service Providers (CSPs)

CSPs issue or register Subscriber authenticators and issue electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use. Primary requirements for CSPs include the following:

- Validate Identity Assertions that are submitted by IdPs as part of a service request
- Define Attributes that IdPs must present for access to the service
- Respond to receipt of various requestor Assertions based on the established policy
- Perform audits on maintained Credentials and make audit information available to the Federation, upon request

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Verifiers

Verifiers confirm the Claimant’s Identity by verifying the Claimant’s possession and control of one or more Authenticators using an authentication protocol. Primary requirements for Verifiers include the following:

- Develop and implement a process to validate Credentials linking Authenticator(s) to a Subscriber’s Identity
- Perform ongoing monitoring of Subscriber Authenticator(s)
- Perform audits on verification events and make audit information available to the Federation, upon request

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Relying Parties

RPs accept the Subscriber’s Authenticator(s) and Credentials or a Verifier’s Assertion of a Claimant’s Identity, typically to process a transaction or grant access to information, network, or Information System. Primary requirements for RPs include the following:

- Define policies featuring factors used in access control or authorization decisions
- Document authorization requirements based on governing Assurance Model
- Perform audits on maintained authorization events and make audit information available to the Federation, upon request

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1463 In addition, certain registration, identity proofing, and issuance processes performed by the
1464 credential service provider (CSP) may be delegated to an entity known as the registration
1465 authority (RA) or identity manager (IM). A close relationship between the RA/IM and CSP is
1466 typical, and the nature of this relationship may differ among RAs, IMs, and CSPs. The minimum
1467 specifications defined in this document assume that relationships between participants and
1468 their requirements are established in the trust framework for the identity management system.

1469
1470 Electronic authentication begins with registration (also referred to as enrollment). The usual
1471 sequence for registration proceeds as follows. An applicant applies to a CSP. If approved, the
1472 CSP creates a credential and binds it to one or more authenticators. The credential includes an
1473 identifier, which can be pseudonymous, and one or more attributes that the CSP has verified.
1474 The authenticators may be issued by the CSP, generated/provided directly by the subscriber, or
1475 provided by a third party. The authenticator and credential may be used in subsequent
1476 authentication events.

1477
1478 The process used to verify an applicant's association with their real world identity is called
1479 identity proofing. The strength of identity proofing is described by a categorization called the
1480 identity assurance level (IAL, see subsection on Assurance Level Model below in this document).
1481 Minimum specifications for identity proofing and verification during the registration process
1482 have been established in *ITRM Guidance Document: Identity Proofing and Verification*.

1483
1484 At IAL 1, identity proofing is not required, therefore any attribute information provided by the
1485 subscriber is self-asserted and not verified. At IAL 2 and 3, identity proofing is required, but the
1486 CSP may assert verified attribute values, verified attribute claims, pseudonymous identifiers, or
1487 nothing. This information assists Relying Parties (RPs) in making access control or authorization
1488 decisions. RPs may decide that their required IAL is 2 or 3, but may only need specific
1489 attributes, and perhaps attributes that retain an individual's pseudonymity. A relying party may
1490 also employ a federated identity approach where the RP outsources all identity proofing,
1491 attribute collection, and attribute storage to a CSP.

1492
1493 In these minimum specifications, the party to be authenticated is called a claimant and the
1494 party verifying that identity is called a verifier. When a claimant successfully demonstrates
1495 possession and control of one or more authenticators to a verifier through an authentication
1496 protocol, the verifier can verify that the claimant is a valid subscriber. The verifier passes on an
1497 assertion about the subscriber, who may be either pseudonymous or non-pseudonymous, to
1498 the RP. That assertion includes an identifier, and may include identity information about the
1499 subscriber, such as the name, or other attributes that were verified in the enrollment process
1500 (subject to the policies of the CSP and the trust framework for the system). When the verifier is
1501 also the RP, the assertion may be implicit. The RP can use the authenticated information
1502 provided by the verifier to make access control or authorization decisions.

1503
1504 Authentication establishes confidence in the claimant's identity, and in some cases in the
1505 claimant's attributes. Authentication does not determine the claimant's authorizations or
1506 access privileges; this is a separate decision. RPs will use a subscriber's authenticated identity

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1507 and attributes with other factors to make access control or authorization decisions. Nothing in
1508 this document precludes RPs from requesting additional information from a subscriber that has
1509 successfully authenticated.

1510
1511 The strength of the authentication process is described by a categorization called the
1512 authenticator assurance level (AAL). AAL 1 requires single-factor authentication and is
1513 permitted with a variety of different authenticator types. At AAL 2, authentication requires two
1514 authentication factors for additional security. Authentication at the highest level, AAL 3,
1515 requires the use of a hardware-based authenticator and one other factor.

1516
1517 As part of authentication, mechanisms such as device identity or geo-location may be used to
1518 identify or prevent possible authentication false positives. While these mechanisms do not
1519 directly increase the authenticator assurance level, they can enforce security policies and
1520 mitigate risks. In many cases, the authentication process and services will be shared by many
1521 applications and agencies. However, it is the individual agency or application acting as the RP
1522 that shall make the decision to grant access or process a transaction based on the specific
1523 application requirements.

1524 Authentication Components and Process Flows

Formatted: Font: 12 pt

1525
1526
1527 The various entities and interactions that comprise the electronic authentication model defined
1528 in these minimum specifications have been illustrated below in **Figure 1**. The left shows the
1529 enrollment, credential issuance, lifecycle management activities, and the stages an individual
1530 transitions, based on the specific phase of the identity proofing and authentication process.

1531
1532 The authentication process begins with the claimant demonstrating to the verifier possession
1533 and control of an authenticator that is bound to the asserted identity through an authentication
1534 protocol. Once possession and control have been demonstrated, the verifier confirms that the
1535 credential remains valid, usually by interacting with the CSP.

1536
1537 The exact nature of the interaction between the verifier and the claimant during the
1538 authentication protocol contributes to the overall security of the system. Well-designed
1539 protocols can protect the integrity and confidentiality of traffic between the claimant and the
1540 verifier both during and after the authentication exchange, and it can help limit the damage
1541 that can be done by an attacker masquerading as a legitimate verifier.

1542
1543 Additionally, mechanisms located at the verifier can mitigate online guessing attacks against
1544 lower entropy secrets like passwords and PINs by limiting the rate at which an attacker can
1545 make authentication attempts or otherwise delaying incorrect attempts. Generally, this is done
1546 by keeping track of and limiting the number of unsuccessful attempts, since the premise of an
1547 online guessing attack is that most attempts will fail.

1548
1549 The verifier is a functional role, but is frequently implemented in combination with the CSP
1550 and/or the RP. If the verifier is a separate entity from the CSP, it is often desirable to ensure

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1551 that the verifier does not learn the subscriber's authenticator secret in the process of
1552 authentication, or at least to ensure that the verifier does not have unrestricted access to
1553 secrets stored by the CSP.

1554 The usual sequence of interactions in the authentication process is as follows:

- 1555 1. An applicant applies to a CSP through a registration process.
- 1556 2. The CSP identity proofs that applicant. Upon successful proofing, the applicant becomes
1557 a subscriber.
- 1558 3. An authenticator and a corresponding credential are established between the CSP and
1559 the new subscriber.
- 1560 4. The CSP maintains the credential, its status, and the enrollment data collected for the
1561 lifetime of the credential. The subscriber maintains his or her authenticator.

1562
1563 Other sequences are less common, but could also achieve the same functional requirements.
1564 The right side of Figure 1 shows the entities and the interactions related to using an
1565 authenticator to perform electronic authentication. When the subscriber needs to authenticate
1566 to perform a transaction, he or she becomes a claimant to a verifier. The interactions are as
1567 follows:

- 1568 1. The claimant proves to the verifier that he or she possesses and controls the
1569 authenticator through an authentication protocol.
- 1570 2. The verifier interacts with the CSP to validate the credential that binds the subscriber's
1571 identity to his or her authenticator and to optionally obtain claimant attributes.
- 1572 3. If the verifier is separate from the RP (application), the verifier provides an assertion
1573 about the subscriber to the RP, which may use the information in the assertion to make
1574 an access control or authorization decision.
- 1575 4. An authenticated session is established between the subscriber and the RP.

1576
1577 In all cases, the RP should request the attributes it requires from a CSP prior to authentication
1578 of the claimant. In addition, the claimant should be requested to consent to the release of
1579 those attributes prior to generation and release of an assertion.

1580
1581 In some cases, the verifier does not need to communicate in real time with the CSP to complete
1582 the authentication activity (e.g., some uses of digital certificates). Therefore, the dashed line
1583 between the verifier and the CSP represents a logical link between the two entities rather than
1584 a physical link. In some implementations, the verifier, RP and the CSP functions may be
1585 distributed and separated as shown in Figure 1; however, if these functions reside on the same
1586 platform, the interactions between the components are local messages between applications
1587 running on the same system rather than protocols over shared untrusted networks.

1588
1589 As noted above, CSPs maintain status information about issued credentials. CSPs may assign a
1590 finite lifetime to a credential in order to limit the maintenance period. When the status
1591 changes, or when the credentials near expiration, credentials may be renewed or re-issued; or,
1592 the credential may be revoked or destroyed. Typically, the subscriber authenticates to the CSP
1593 using his or her existing, unexpired authenticator and credential in order to request issuance of
1594

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

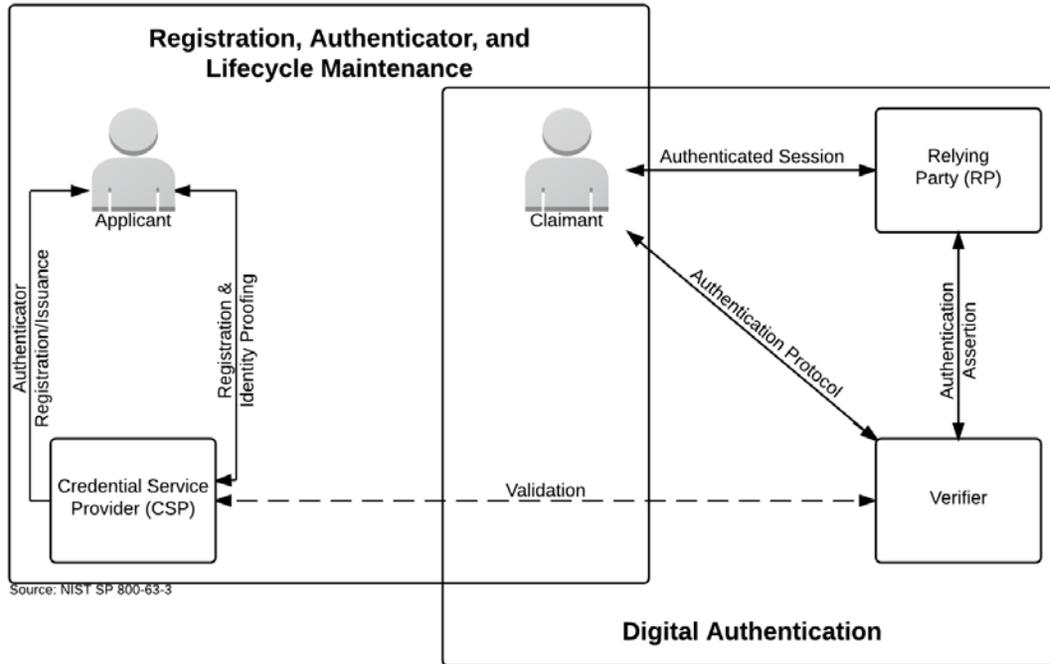
1595 | a new authenticator and credential. If the subscriber fails to request authenticator and
1596 | credential re-issuance prior to their expiration or revocation, he or she may be required to
1597 | repeat the enrollment process to obtain a new authenticator and credential. Alternatively, the
1598 | CSP may choose to accept a request during a grace period after expiration.

DRAFT

Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1599

Figure 1. Electronic Authentication Model



1600
1601
1602
1603
1604
1605
1606
1607
1608

Source: NIST SP 800-63-3, accessible at <https://pages.nist.gov/800-63-3/sp800-63-3.html>

Note: Figure 1 illustrates the model for electronic authentication in an identity management system, as documented in NIST SP 800-63-3 (Public Review), containing all components, requirements, and specifications recommended by IMSAC. However, the minimum specifications defined in this document have been developed to accommodate requirements for electronic authentication established under other national and international standards.

Formatted: Font: 12 pt

Formatted: Default Paragraph Font, Font: 12 pt

1609 Authentication Protocols and Lifecycle Management

1610
1611 Authenticators

1612 The established paradigm for electronic authentication identifies three factors as the
1613 cornerstone of authentication:

- 1614 ■ Something you know (for example, a password)
- 1615 ■ Something you have (for example, an ID badge or a cryptographic key)
- 1616 ■ Something you are (for example, a fingerprint or other biometric data)

1617
1618 Multi-factor authentication refers to the use of more than one of the factors listed above. The
1619 strength of authentication systems is largely determined by the number of factors incorporated
1620 by the system. Implementations that use two different factors are considered to be stronger
1621 than those that use only one factor; systems that incorporate all three factors are stronger than
1622 systems that only incorporate two of the factors. Other types of information, such as location
1623 data or device identity, may be used by an RP or verifier to evaluate the risk in a claimed
1624 identity, but they are not considered authentication factors.

1625
1626 In electronic authentication the claimant possesses and controls one or more authenticators
1627 that have been registered with the CSP and are used to prove the claimant's identity. The
1628 authenticator(s) contains secrets the claimant can use to prove that he or she is a valid
1629 subscriber, the claimant authenticates to a system or application over a network by proving
1630 that he or she has possession and control of an authenticator.

1631
1632 The secrets contained in authenticators are based on either public key pairs (asymmetric keys)
1633 or shared secrets (symmetric keys). A public key and a related private key comprise a public key
1634 pair. The private key is stored on the authenticator and is used by the claimant to prove
1635 possession and control of the authenticator. A verifier, knowing the claimant's public key
1636 through some credential (typically a public key certificate), can use an authentication protocol
1637 to verify the claimant's identity, by proving that the claimant has possession and control of the
1638 associated private key authenticator.

1639
1640 Shared secrets stored on authenticators may be either symmetric keys or passwords. While
1641 they can be used in similar protocols, one important difference between the two is how they
1642 relate to the subscriber. While symmetric keys are generally stored in hardware or software
1643 that the subscriber controls, passwords are intended to be memorized by the subscriber. As
1644 such, keys are something the subscriber has, while passwords are something he or she knows.
1645 Since passwords are committed to memory, they usually do not have as many possible values
1646 as cryptographic keys, and, in many protocols, are severely vulnerable to network attacks that
1647 are more restricted for keys.

1648
1649 Moreover, the entry of passwords into systems (usually through a keyboard) presents the
1650 opportunity for very simple keyboard logging attacks, and may also allow those nearby to learn
1651 the password by watching it being entered. Therefore, keys and passwords demonstrate
1652 somewhat separate authentication properties (something you have rather than something you

1653 know). When using either public key pairs or shared secrets, the subscriber has a duty to
1654 maintain exclusive control of his or her authenticator, since possession and control of the
1655 authenticator is used to authenticate the claimant's identity.

1656
1657 The minimum specifications defined in this document assume that authenticators always
1658 contain a secret. Authentication factors classified as something you know are not necessarily
1659 secrets. Knowledge-based authentication, where the claimant is prompted to answer questions
1660 that can be confirmed from public databases, also does not constitute an acceptable secret for
1661 electronic authentication. More generally, something you are does not generally constitute a
1662 secret. However, the requirements for some identity management systems may allow the use
1663 of biometrics as an authenticator.

1664
1665 Biometric characteristics are unique personal attributes that can be used to verify the identity
1666 of a person who is physically present at the point of verification. They include facial features,
1667 fingerprints, iris patterns, voiceprints, and many other characteristics. NIST recommends that
1668 biometrics be used in the enrollment process for higher levels of assurance to later help
1669 prevent a subscriber who is registered from repudiating the enrollment, to help identify those
1670 who commit enrollment fraud, and to unlock authenticators. The specific requirements for the
1671 use of biometrics must be defined in the trust framework for the system.

1672
1673 The minimum specifications in this document encourage identity management systems to use
1674 authentication processes and protocols that incorporate all three factors, as a means of
1675 enhancing system security. An electronic authentication system may incorporate multiple
1676 factors in either of two ways. The system may be implemented so that multiple factors are
1677 presented to the verifier, or some factors may be used to protect a secret presented to the
1678 verifier. If multiple factors are presented to the verifier, each will need to be an authenticator
1679 (and therefore contain a secret). If a single factor is presented to the verifier, the additional
1680 factors are used to protect the authenticator and need not themselves be authenticators.

1681 Credentials

1682 As described in the preceding sections, credentials bind an authenticator to the subscriber as
1683 part of the issuance process. Credentials are stored and maintained by the CSP. The claimant
1684 possesses an authenticator, but is not necessarily in possession of the electronic credentials.
1685 For example, database entries containing the user attributes are considered to be credentials
1686 for the purpose of this document but are possessed by the verifier.

1687 Assertions

1688
1689 Upon completion of the electronic authentication process, the verifier generates an assertion
1690 containing the result of the authentication and provides it to the RP. If the verifier is
1691 implemented in combination with the RP, the assertion is implicit. If the verifier is a separate
1692 entity from the RP, as in typical federated identity models, the assertion is used to
1693 communicate the result of the authentication process, and optionally information about the
1694 subscriber, from the verifier to the RP.
1695

1696 Assertions may be communicated directly to the RP, or can be forwarded through the
1697 subscriber, which has further implications for system design. An RP trusts an assertion based
1698 on the source, the time of creation, and the corresponding trust framework that governs the
1699 policies and process of CSPs and RPs. The verifier is responsible for providing a mechanism by
1700 which the integrity of the assertion can be confirmed.

1701
1702 The RP is responsible for authenticating the source (e.g., the verifier) and for confirming the
1703 integrity of the assertion. When the verifier passes the assertion through the subscriber, the
1704 verifier must protect the integrity of the assertion in such a way that it cannot be modified by
1705 the subscriber. However, if the verifier and the RP communicate directly, a protected session
1706 may be used to provide the integrity protection. When sending assertions across a network, the
1707 verifier is responsible for ensuring that any sensitive subscriber information contained in the
1708 assertion can only be extracted by an RP that it trusts to maintain the information's
1709 confidentiality.

1710
1711 Examples of assertions include:

- 1712 • SAML Assertions – SAML assertions are specified using a mark-up language intended for
1713 describing security assertions. They can be used by a verifier to make a statement to an
1714 RP about the identity of a claimant. SAML assertions may be digitally signed.
- 1715 • OpenID Connect Claims – OpenID Connect are specified using JavaScript Object Notation
1716 (JSON) for describing security, and optionally, user claims. JSON user info claims may be
1717 digitally signed.
- 1718 • Kerberos Tickets – Kerberos Tickets allow a ticket granting authority to issue session
1719 keys to two authenticated parties using symmetric key based encapsulation schemes.

1720
1721 **Relying Parties**

1722 An RP relies on results of an authentication protocol to establish confidence in the identity or
1723 attributes of a subscriber for the purpose of conducting an online transaction. RPs may use a
1724 subscriber's authenticated identity (pseudonymous or non-pseudonymous), the IAL, AAL, and
1725 other factors to make access control or authorization decisions. The verifier and the RP may be
1726 the same entity, or they may be separate entities. If they are separate entities, the RP normally
1727 receives an assertion from the verifier. The RP ensures that the assertion came from a verifier
1728 trusted by the RP. The RP also processes any additional information in the assertion, such as
1729 personal attributes or expiration times.

1730
1731

Formatted: Font: 12 pt, Not Bold

Formatted: Font: Not Bold

Formatted: Font: 12 pt, Not Bold

1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769

Assurance Model

The minimum specifications defined in this document for electronic authentication assume that the trust framework for an identity management system will define a specific assurance model for that system.⁴⁴ Therefore, the assurance model presented below, which is based on NIST SP 800-63-3, should be viewed as a recommended framework for electronic authentication. Other assurance models have been established in OMB M-04-04 and the State Identity, Credential, and Access Management (SICAM) guidelines, published by the National Association of Chief Information Officers (NASCIO). A crosswalk showing disparities in the NIST SP 800-63-3, OMB M-04-04, and SICAM assurance models has been provided in **Figure 2**.

Identity Assurance Level 1—At this level, attributes provided in conjunction with the authentication process, if any, are self-asserted.

Identity Assurance Level 2—IAL 2 introduces the need for either remote or in-person identity proofing. IAL 2 requires identifying attributes to have been verified in-person or remotely using, at a minimum, the procedures given in NIST 800-63A.

Identity Assurance Level 3—At IAL 3, in-person identity proofing is required. Identifying attributes must be verified by an authorized representative of the CSP through examination of physical documentation as described in NIST 800-63A.

Authenticator Assurance Level 1—AAL 1 provides single factor electronic authentication, giving some assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. AAL 1 allows a wide range of available authentication technologies to be employed and requires only a single authentication factor to be used. It also permits the use of any of the authentication methods of higher authenticator assurance levels. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she possesses and controls the authenticator.

Authenticator Assurance Level 2—AAL 2 provides higher assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. Two different authentication factors are required. Various types of authenticators, including multi-factor Software Cryptographic Authenticators, may be used as described in NIST 800-63B. AAL 2 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires cryptographic mechanisms that protect the primary authenticator against compromise by the protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved cryptographic techniques are required for all assertion protocols used at AAL 2 and above.⁴⁵

⁴⁴ Trust Framework Identity Trust Frameworks for identity management system Digital Identity Systems also should set requirements for how the assurance for each credential will be documented in the metadata for the credential to support audit and compliance.

⁴⁵ Approved cryptographic techniques shall must be FIPS approved, NIST recommended, or otherwise compliant with Commonwealth IT Information Security Standard (SEC501);

Formatted: Font: Not Bold

Formatted: Normal

1770 Authenticator Assurance Level 3 – AAL 3 is intended to provide the highest practical electronic
 1771 authentication assurance. Authentication at AAL 3 is based on proof of possession of a key
 1772 through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only “hard”
 1773 cryptographic authenticators are allowed. The authenticator is required to be a hardware
 1774 cryptographic module validated at Federal Information Processing Standard (FIPS) 140 Level 2
 1775 or higher overall with at least FIPS 140 Level 3 physical security. AAL 3 authenticator
 1776 requirements can be met by using the PIV authentication key of a FIPS 201 compliant Personal
 1777 Identity Verification (PIV) Card.

1778 **Figure 2. Assurance Model Crosswalk**

OMB M04-04 Level of Assurance	SICAM Assurance Level	NIST SP 800-63-3 IAL	NIST SP 800-63-3 AAL
1	1	1	1
2	2	2	2 or 3
3	3	2	2 or 3
4	4	3	3

Formatted: Font: 12 pt

1781

1782 **Privacy and Security**

1783

1784 The minimum specifications established in this document for privacy and security in the use of
 1785 person information for ~~electronic authentication~~ [Electronic Authentication](#) apply the Fair
 1786 Information Practice Principles (FIPPs).¹⁶ The FIPPs have been endorsed by the National
 1787 Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.¹⁷

1788

1789 The minimum specifications also adhere to the Identity Ecosystem Framework (IDEF) Baseline
 1790 Functional Requirements (v.1.0) for privacy and security, adopted by the Identity Ecosystem
 1791 Steering Group (IDESG) in October 2015 (**Appendix 2**).

1792

1793 The minimum specifications for ~~identity proofing~~ [Assertions and verification](#) apply the following
 1794 FIPPs:

- 1795 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants
 1796 regarding collection, use, dissemination, and maintenance of person information required
 1797 during the ~~registration~~ [Registration](#), ~~identity proofing~~ [Identity Proofing](#) and verification
 1798 processes.
- 1799 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using
 1800 person information and, to the extent practicable, seek consent for the collection, use,
 1801 dissemination, and maintenance of that information. RAs and CSPs also should provide
 1802 mechanisms for appropriate access, correction, and redress of person information.
- 1803 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits
 1804 the collection of person information and specifically articulate the purpose or purposes for
 1805 which the information is intended to be used.
- 1806 • Data Minimization: RAs and CSPs should collect only the person information directly
 1807 relevant and necessary to accomplish the ~~registration~~ [Registration](#) and related processes,
 1808 and only retain that information for as long as necessary to fulfill the specified purpose.
- 1809 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for
 1810 the purpose specified in the notice. Disclosure or sharing that information should be limited
 1811 to the specific purpose for which the information was collected.
- 1812 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that
 1813 person information is accurate, relevant, timely, and complete.
- 1814 • Security: RAs and CSPs should protect personal information through appropriate security
 1815 safeguards against risks such as loss, unauthorized access or use, destruction, modification,
 1816 or unintended or inappropriate disclosure.

¹⁶ The term “person information” refers to protected data for person entities, governed by Applicable Law. This includes Personally Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), Protected Education Records, and related categories. Specific requirements for the privacy and security of person information should be defined by the ~~trust framework~~ [Identity Trust Framework](#) for the ~~identity management system~~ [Digital Identity System](#).

¹⁷ The FIPPs endorsed by NSTIC may be accessed at <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf>. The FIPPs published in SICAM may be accessed at <http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf>.

1817 Accountability and Auditing: RAs and CSPs should be accountable for complying with these
1818 principles, providing training to all employees and contractors who use person information,
1819 and auditing the actual use of person information to demonstrate compliance with these
1820 principles and all applicable privacy protection requirements.

1821 **7 Alignment Comparison**

Formatted: Font: Bold, Font color: Text 1

Formatted: List Paragraph

~~The minimum specifications for electronic authentication defined in this document have been developed to align with existing national and international standards for electronic authentication and identity management. Specifically, the minimum specifications reflect basic requirements set forth in national standards at the federal and state level, ensuring compliance while accommodating other identity management standards and protocols. This document assumes that each identity management system will comply with those governing standards and protocols required by Applicable Law.~~

~~The following section outlines the alignment and disparities between the minimum specifications in this document and core national standards. A crosswalk documenting the alignment and areas of misalignment has been provided in Appendix 3.~~

1835 **NIST SP 800-63-3**

~~The minimum specifications in this document conform with the basic requirements for electronic authentication set forth in NIST SP 800-63-3 (Public Review version). However, as the NIST guidance defines specific requirements for federal agencies, the minimum specifications in this document provide flexibility for identity management systems across industries in the private sector and levels of governance. This flexibility enables identity management systems to adhere to the specifications but do so in a manner appropriate and compliant with their governing trust frameworks.~~

1845 **State Identity and Access Management Credential (SICAM) Guidance and Roadmap**

~~The minimum specifications in this document conform with the basic requirements for electronic authentication set forth by NASCIO in the SICAM Guidance and Roadmap. The NASCIO guidance defines specific requirements for state agencies. Similar to the contrast with the NIST guidance for federal agencies, the minimum specifications in this document provide flexibility for identity management systems across industries in the private sector and levels of governance.~~

1854 **IDESG Identity Ecosystem Framework (IDEF) Functional Model**

~~The minimum specifications in this document conform with the core operations and basic requirements for privacy and security set forth by IDESG in the IDEF Functional Model and Baseline Functional Requirements. The IDESG/IDEF requirements apply the FIPPs but extend them to cover the Guiding Principles of the National Strategy for~~

1860
1861
1862
1863

Trusted Identities in Cyberspace (NSTIC). The minimum specifications in this document encourage adherence to the IDEF Functional Model, Baseline Functional Requirements and the NSTIC Guiding Principles.

Formatted: List Paragraph, Indent: Left: 0", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

DRAFT

1864 Appendix 1. IMSAC Charter

1865
1866
1867
1868
1869

COMMONWEALTH OF VIRGINIA
IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL
CHARTER

1870 **Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)**1871
1872
1873
1874
1875

The Identity Management Standards Advisory Council (the Advisory Council) advises the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to § 2.2-436.

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an [identity-Identity](#) Trust Framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third [partiesParticipants](#) on identity credentials, as defined in § 59.1-550.

1883
1884
1885**Membership and Governance Structure (§ 2.2-437.B)**

The Advisory Council's membership and governance structure is as follows:

- 1887 1. The Advisory Council consists of seven members, to be appointed by the Governor, with
1888 expertise in electronic identity management and information technology. Members include
1889 a representative of the Department of Motor Vehicles, a representative of the Virginia
1890 Information Technologies Agency, and five representatives of the business community with
1891 appropriate experience and expertise. In addition to the seven appointed members, the
1892 Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex
1893 officio member of the Advisory Council.
- 1894 2. The Advisory Council designates one of its members as chairman.
- 1895 3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure
1896 of the Governor, and may be reappointed.
- 1897 4. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure
1898 of the Governor, and may be reappointed.
- 1899 5. Members serve without compensation but may be reimbursed for all reasonable and
1900 necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.
- 1901 6. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

1902
1903
1904
1905

1906 The formation, membership and governance structure for the Advisory Council has been
1907 codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

1908
1909 The statutory authority and requirements for public notice and comment periods for guidance
1910 documents have been established pursuant to § 2.2-437.C, as follows:

1911
1912 C. Proposed guidance documents and general opportunity for oral or written submittals as to
1913 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published
1914 in the Virginia Register of Regulations as a general notice following the processes and
1915 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§
1916 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written
1917 comments following the posting and publication and shall hold at least one meeting dedicated
1918 to the receipt of oral comment no less than 15 days after the posting and publication. The
1919 Advisory Council shall also develop methods for the identification and notification of interested
1920 partiesParticipants and specific means of seeking input from interested persons and groups.

1921 The Advisory Council shall send a copy of such notices, comments, and other background
1922 material relative to the development of the recommended guidance documents to the Joint
1923 Commission on Administrative Rules.

1924
1925
1926 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the
1927 minutes of the meeting and related IMSAC documents, visit:
1928 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

1929 Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline 1930 Functional Requirements (v.1.0) for Privacy and Security

1931

1932 PRIVACY-1. DATA MINIMIZATION

1933 Entities MUST limit the collection, use, transmission and storage of personal information to the
1934 minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities
1935 providing claims or attributes MUST NOT provide any more personal information than what is
1936 requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to
1937 accommodate information requests of variable granularity, to support data minimization.

1938

1939 PRIVACY-2. PURPOSE LIMITATION

1940 Entities MUST limit the use of personal information that is collected, used, transmitted, or
1941 stored to the specified purposes of that transaction. Persistent records of contracts, assurances,
1942 consent, or legal authority MUST be established by entities collecting, generating, using,
1943 transmitting, or storing personal information, so that the information, consistently is used in
1944 the same manner originally specified and permitted.

1945

1946 PRIVACY-3. ATTRIBUTE MINIMIZATION

1947 Entities requesting attributes MUST evaluate the need to collect specific attributes in a
1948 transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST
1949 collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever
1950 feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities
1951 MUST be bound to claims instead of actual attribute values.

1952

1953 PRIVACY-4. CREDENTIAL LIMITATION

1954 Entities MUST NOT request USERS' credentials unless necessary for the transaction and then
1955 only as appropriate to the risk associated with the transaction or to the risks to the
1956 [parties/Participants](#) associated with the transaction.

1957

1958 PRIVACY-5. DATA AGGREGATION RISK

1959 Entities MUST assess the privacy risk of aggregating personal information, in systems and
1960 processes where it is collected, generated, used, transmitted, or stored, and wherever feasible,
1961 MUST design and operate their systems and processes to minimize that risk. Entities MUST
1962 assess and limit linkages of personal information across multiple transactions without the
1963 USER's explicit consent.

1964

1965 PRIVACY-6. USAGE NOTICE

1966 Entities MUST provide concise, meaningful, and timely communication to USERS describing how
1967 they collect, generate, use, transmit, and store personal information.

1968

1969 PRIVACY-7. USER DATA CONTROL

1970 Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete
1971 personal information.

1972 PRIVACY-8. THIRD-PARTY LIMITATIONS

1973 Wherever USERS make choices regarding the treatment of their personal information, those
1974 choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it
1975 transmits the personal information.

1976
1977 PRIVACY-9. USER NOTICE OF CHANGES

1978 Entities MUST, upon any material changes to a service or process that affects the prior or
1979 ongoing collection, generation, use, transmission, or storage of USERS' personal information,
1980 notify those USERS, and provide them with compensating controls designed to mitigate privacy
1981 risks that may arise from those changes, which may include seeking express affirmative consent
1982 of USERS in accordance with relevant law or regulation.

1983
1984 PRIVACY-10. USER OPTION TO DECLINE

1985 | USERS MUST have the opportunity to decline ~~registration~~Registration; decline credential
1986 provisioning; decline the presentation of their credentials; and decline release of their
1987 attributes or claims.

1988
1989 PRIVACY-11. OPTIONAL INFORMATION

1990 Entities MUST clearly indicate to USERS what personal information is mandatory and what
1991 information is optional prior to the transaction.

1992
1993 PRIVACY-12. ANONYMITY

1994 Wherever feasible, entities MUST utilize identity systems and processes that enable
1995 transactions that are anonymous, anonymous with validated attributes, pseudonymous, or
1996 where appropriate, uniquely identified. Where applicable to such transactions, entities
1997 employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES
1998 collecting USER personal information. Organizations MUST request individuals' credentials only
1999 when necessary for the transaction and then only as appropriate to the risk associated with the
2000 | transaction or only as appropriate to the risks to the ~~parties~~Participants associated with the
2001 transaction.

2002
2003 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

2004 Controls on the processing or use of USERS' personal information MUST be commensurate with
2005 the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by
2006 entities who conduct digital identity management functions, to establish what risks those
2007 functions pose to USERS' privacy.

2008
2009 PRIVACY-14. DATA RETENTION AND DISPOSAL

2010 Entities MUST limit the retention of personal information to the time necessary for providing
2011 and administering the functions and services to USERS for which the information was collected,
2012 except as otherwise required by law or regulation. When no longer needed, personal
2013 information MUST be securely disposed of in a manner aligning with appropriate industry
2014 standards and/or legal requirements.

2015

2016 PRIVACY-15. ATTRIBUTE SEGREGATION

2017 Wherever feasible, identifier data MUST be segregated from attribute data.

2018 SECURE-1. SECURITY PRACTICES

2019 Entities MUST apply appropriate and industry-accepted information security STANDARDS,
2020 guidelines, and practices to the systems that support their identity functions and services.

2021

2022 SECURE-2. DATA INTEGRITY

2023 Entities MUST implement industry-accepted practices to protect the confidentiality and
2024 integrity of identity data—including authentication data and attribute values—during the
2025 execution of all digital identity management functions, and across the entire data lifecycle
2026 (collection through destruction).

2027

2028 SECURE-3. CREDENTIAL REPRODUCTION

2029 Entities that issue or manage credentials and tokens MUST implement industry-accepted
2030 processes to protect against their unauthorized disclosure and reproduction.

2031

2032 SECURE-4. CREDENTIAL PROTECTION

2033 Entities that issue or manage credentials and tokens MUST implement industry-accepted data
2034 integrity practices to enable individuals and other entities to verify the source of credential and
2035 token data.

2036

2037 SECURE-5. CREDENTIAL ISSUANCE

2038 Entities that issue or manage credentials and tokens MUST do so in a manner designed to
2039 assure that they are granted to the appropriate and intended USER(s) only. Where
2040 ~~registration~~[Registration](#) and credential issuance are executed by separate entities, procedures
2041 for ensuring accurate exchange of ~~registration~~[Registration](#) and issuance information that are
2042 commensurate with the stated assurance level MUST be included in business agreements and
2043 operating policies.

2044

2045 SECURE-6. CREDENTIAL UNIQUENESS

2046 Entities that issue or manage credentials MUST ensure that each account to credential pairing is
2047 uniquely identifiable within its namespace for authentication purposes.

2048

2049 SECURE-7. TOKEN CONTROL

2050 Entities that authenticate a USER MUST employ industry-accepted secure authentication
2051 protocols to demonstrate the USER's control of a valid token.

2052

2053 SECURE-8. MULTIFACTOR AUTHENTICATION

2054 Entities that authenticate a USER MUST offer authentication mechanisms which augment or are
2055 alternatives to a password.

2056

2057 SECURE-9. AUTHENTICATION RISK ASSESSMENT

2058 Entities MUST have a risk assessment process in place for the selection of authentication
2059 mechanisms and supporting processes.

2060
2061
2062
2063 SECURE-10. UPTIME
2064 Entities that provide and conduct digital identity management functions MUST have established
2065 policies and processes in place to maintain their stated assurances for availability of their
2066 services.
2067
2068 SECURE-11. KEY MANAGEMENT
2069 Entities that use cryptographic solutions as part of identity management MUST implement key
2070 management policies and processes that are consistent with industry-accepted practices.
2071
2072 SECURE-12. RECOVERY AND REISSUANCE
2073 Entities that issue credentials and tokens MUST implement methods for reissuance, updating,
2074 and recovery of credentials and tokens that preserve the security and assurance of the original
2075 ~~registration~~[Registration](#) and credentialing operations.
2076
2077 SECURE-13. REVOCATION
2078 Entities that issue credentials or tokens MUST have processes and procedures in place to
2079 invalidate credentials and tokens.
2080
2081 SECURE-14. SECURITY LOGS
2082 Entities conducting digital identity management functions MUST log their transactions and
2083 security events, in a manner that supports system audits and, where necessary, security
2084 investigations and regulatory requirements. Timestamp synchronization and detail of logs
2085 MUST be appropriate to the level of risk associated with the environment and transactions.
2086
2087 SECURE-15. SECURITY AUDITS
2088 Entities MUST conduct regular audits of their compliance with their own information security
2089 policies and procedures, and any additional requirements of law, including a review of their
2090 logs, incident reports and credential loss occurrences, and MUST periodically review the
2091 effectiveness of their policies and procedures in light of that data.
2092

DRAFT

2094

Appendix 3. Electronic Authentication Standards Alignment Comparison Matrix

Component	NIST 800-63-3 (Public Review)	SICAM	IDESG IDEF Functional Model
Registration	Alignment: Defines protocols and process flows for applicant registration with a federal agency through an RA, IM or CSP	Alignment: Defines protocols and process flows for applicant registration with a state agency through an RA, IM or CSP	Alignment: Identifies core operations within standard registration process flows
	Misalignment: Federal protocols for applicant registration with federal agencies may not be appropriate across sectors or private industry	Misalignment: State protocols for applicant registration with state agencies may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria for applicant registration
Identity Proofing & Verification	Alignment: Establishes rigorous requirements for identity proofing and verification by federal agencies	Alignment: Establishes rigorous requirements for identity proofing and verification by state agencies	Alignment: Defines core operations for identity proofing and verification
	Misalignment: Federal requirements for identity proofing and verification may not be appropriate across sectors or private industry	Misalignment: SICAM model identity proofing and verification may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria for acceptable identity proofing and verification
Authenticators & Credentials	Alignment: Sets protocols and required flows for federal agencies to follow in issuing, maintaining and deprecating authenticators and credentials	Alignment: Sets protocols and required flows for state agencies to follow in issuing, maintaining and deprecating authenticators (tokens) and credentials	Alignment: Documents core operations for authenticators (tokens) and credentials
	Misalignment: Federal protocols for authenticators and credentials may not be appropriate across sectors or private industry	Misalignment: SICAM model for authenticators and credentials may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria for authenticators (tokens) and credentials
Authentication Protocols & Assertions	Alignment: Provides clearly defined technical requirements for authentication protocols and assertions for federal agencies	Alignment: Provides clearly defined technical requirements for authentication protocols and assertions for state agencies	Alignment: Defines core operations for authentication protocols and assertions
	Misalignment: Federal authentication protocols and assertions may not be appropriate across sectors or private industry	Misalignment: SICAM model authentication protocols and assertions may not be appropriate across sectors or private industry	Misalignment: Core operational definitions do not contain specific criteria or technical requirements for authentication protocols and assertions
Role-Based Requirements for Authentication (RAs, CSPs, RPs, Verifiers)	Alignment: Establishes role-based requirements for federal agencies, RAs, CSPs, RPs, and Verifiers	Alignment: Establishes role-based requirements for state agencies, RAs, CPS, RPs, and Verifiers	Alignment: Identifies core, role-based operational requirements for RAs, CSPs, RPs, and Verifiers
	Misalignment: Federal role-based requirements may not be appropriate across sectors or private industry	Misalignment: State role-based requirements may not be appropriate across sectors or private industry	Misalignment: Core operational roles and responsibilities do not contain specific criteria for role-based requirements

- Formatted: Normal, Tab stops: 1", Left
- Formatted: Width: 8.5", Height: 11", Numbering: Continuous
- Formatted: Left, Space Before: 0 pt, After: 0 pt, Tab stops: 1", Left
- Formatted: Left, Tab stops: 1", Left
- Formatted: Tab stops: 1", Left
- Formatted: Tab stops: 1", Left
- Formatted: Left, Tab stops: 1", Left
- Formatted: Tab stops: 1", Left
- Formatted: Tab stops: 1", Left
- Formatted: Left, Tab stops: 1", Left
- Formatted: Tab stops: 1", Left
- Formatted: Tab stops: 1", Left
- Formatted: Left, Tab stops: 1", Left
- Formatted: Tab stops: 1", Left
- Formatted: Left, Space Before: 0 pt, After: 0 pt, Tab stops: 1", Left
- Formatted: Tab stops: 1", Left
- Formatted: Left, Tab stops: 1", Left
- Formatted: Tab stops: 1", Left

2096