

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management (ITRM)

GUIDANCE DOCUMENT

[Digital Identity Electronic Authentication Assertions](#)

Virginia Information Technologies Agency (VITA)

Table of Contents

1	Publication Version Control	1
2	Reviews	1
3	Statutory Authority	2
4	Definitions	3
5	Background	1415
6	Minimum Specifications	1516
7	Alignment Comparison	26

DRAFT

1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	07/20 10/12/2016	Initial Draft of Document

Formatted Table

2 Reviews

~~• The initial version of the document was prepared on behalf of the Identity Management Standards Advisory Council (IMSAC) by the staff analysts for Commonwealth Data Governance, a division of the Enterprise Architecture Directorate of the Virginia Information Technologies Agency. 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.~~

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

~~• The document will be reviewed in a manner compliant with the Commonwealth of Virginia's ITRM Policies, Standards, and Guidelines and §2.2-437.C, Code of Virginia:~~

Formatted: Normal, No bullets or numbering

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

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

DRAFT

3 Statutory Authority

The following section documents the statutory authority established in the *Code of Virginia* for the development of minimum specifications and standards for Assertions within a Digital Identity System. References to statutes below and throughout this document shall be to the *Code of Virginia*, unless otherwise specified.

Governing Statutes:

Secretary of Technology

§ 2.2-225. Position established; agencies for which responsible; additional powers

<http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/>

Secretary of Transportation

§ 2.2-228. Position established; agencies for which responsible

<http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-228/>

Identity Management Standards Advisory Council

§ 2.2-437. Identity Management Standards Advisory Council

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

Commonwealth Identity Management Standards

§ 2.2-436. Approval of electronic identity standards

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

Electronic Identity Management Act

Chapter 50. Electronic Identity Management Act

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

Chief Information Officer (CIO) of the Commonwealth

§ 2.2-2007. Powers of the CIO

<http://law.lis.virginia.gov/vacode/title2.2/chapter20.1/section2.2-2007/>

Virginia Information Technologies Agency

Chapter 20.1. Virginia Information Technologies Agency

<http://law.lis.virginia.gov/vacode/title2.2/chapter20.1/>The following section documents the statutory authority established in the *Code of Virginia* for the development of minimum specifications and standards for electronic authentication. References to statutes below and throughout this document shall be to the *Code of Virginia*, unless otherwise specified.

75 **Governing Statutes:**

76

77 **Secretary of Technology**

78 § 2.2-225. Position established; agencies for which responsible; additional powers

79 <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225>

80

81 **Secretary of Transportation**

82 § 2.2-225. Position established; agencies for which responsible; additional powers

83 <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-225>

84

85 **Identity Management Standards Advisory Council**

86 § 2.2-437. Identity Management Standards Advisory Council

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

88

89 **Commonwealth Identity Management Standards**

90 § 2.2-436. Approval of electronic identity standards

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

92

93 **Electronic Identity Management Act**

94 Chapter 50. Electronic Identity Management Act

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

96

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

98 § 2.2-2007. Powers of the CIO

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

100

101 **Virginia Information Technologies Agency**

102 § 2.2-2010. Additional powers of VITA

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

104

105

106

107

108

109 **4 Definitions**

110

111 Terms used in this document comply with definitions in the Public Review version of the

112 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3).

113 [and align with adopted definitions in § 59.1-550, Code of Virginia \(COV\), and the](#)
114 [Commonwealth of Virginia’s ITRM Glossary \(ITRM Glossary\).](#)¹
115
116 [Active Attack: An online attack where the attacker transmits data to the claimant, credential](#)
117 [service provider, verifier, or relying Participant. Examples of active attacks include man-in-the-](#)
118 [middle, impersonation, and session hijacking.](#)
119
120 [Address of Record: The official location where an individual can be found. The address of record](#)
121 [always includes the residential street address of an individual and may also include the mailing](#)
122 [address of the individual. In very limited circumstances, an Army Post Office box number, Fleet](#)
123 [Post Office box number or the street address of next of kin or of another contact individual can](#)
124 [be used when a residential street address for the individual is not available.](#)
125
126 [Approved: Federal Information Processing Standard \(FIPS\) approved or NIST recommended. An](#)
127 [algorithm or technique that is either 1\) specified in a FIPS or NIST Recommendation, or 2\)](#)
128 [adopted in a FIPS or NIST Recommendation.](#)
129
130 [Applicable Law: Laws, statutes, regulations, and rules of the jurisdiction in which the members](#)
131 [of an Identity Trust Framework operates.](#)
132
133 [Applicant: A Participant undergoing the processes of Registration and Identity Proofing.](#)
134
135 [Assertion: A statement from a verifier to a relying Participant \(RP\) that contains identity](#)
136 [information about a Subscriber. Assertions may also contain verified attributes.](#)
137
138 [Assertion Reference: A data object, created in conjunction with an Assertion, which identifies](#)
139 [the verifier and includes a pointer to the full Assertion held by the verifier.](#)
140
141 [Assurance: In the context of \[OMB M-04-04\]² and this document, assurance is defined as 1\) the](#)
142 [degree of confidence in the vetting process used to establish the identity of an individual to](#)
143 [whom the credential was issued, and 2\) the degree of confidence that the individual who uses](#)
144 [the credential is the individual to whom the credential was issued.](#)
145 [Assurance Model: Policies, processes, and protocols that define how Assurance will be](#)
146 [established in an Identity Trust Framework.](#)
147

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](http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/), 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>.

148 [Asymmetric Keys: Two related keys, a public key and a private key that are used to perform](#)
149 [complementary operations, such as encryption and decryption or signature generation and](#)
150 [signature verification.](#)
151
152 [Attack: An attempt by an unauthorized individual to fool a verifier or a relying Participant into](#)
153 [believing that the unauthorized individual in question is the Subscriber.](#)
154
155 [Attacker: A Participant who acts with malicious intent to compromise an Information System.](#)
156
157 [Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or](#)
158 [something.](#)
159
160 [Authentication: The process of establishing confidence in the identity of users or Information](#)
161 [Systems.](#)
162
163 [Authentication Protocol: A defined sequence of messages between a claimant and a verifier](#)
164 [that demonstrates that the claimant has possession and control of a valid authenticator to](#)
165 [establish his/her identity, and optionally, demonstrates to the claimant that he or she is](#)
166 [communicating with the intended verifier.](#)
167
168 [Authentication Protocol Run: An exchange of messages between a claimant and a verifier that](#)
169 [results in authentication \(or authentication failure\) between the two Participants.](#)
170
171 [Authentication Secret: A generic term for any secret value that could be used by an attacker to](#)
172 [impersonate the Subscriber in an authentication protocol. These are further divided into short-](#)
173 [term authentication secrets, which are only useful to an attacker for a limited period of time,](#)
174 [and long-term authentication secrets, which allow an attacker to impersonate the Subscriber](#)
175 [until they are manually reset. The authenticator secret is the canonical example of a long term](#)
176 [authentication secret, while the authenticator output, if it is different from the authenticator](#)
177 [secret, is usually a short term authentication secret.](#)
178
179 [Authenticator: Something that the claimant possesses and controls \(typically a cryptographic](#)
180 [module or password\) that is used to authenticate the claimant's identity. In previous versions of](#)
181 [this guideline, this was referred to as a token.](#)
182
183 [Authenticator Assurance Level \(AAL\): A metric describing robustness of the authentication](#)
184 [process proving that the claimant is in control of a given Subscriber's authenticator\(s\).](#)
185
186 [Authenticator Output: The output value generated by an authenticator. The ability to generate](#)
187 [valid authenticator outputs on demand proves that the claimant possesses and controls the](#)
188 [authenticator. Protocol messages sent to the verifier are dependent upon the authenticator](#)
189 [output, but they may or may not explicitly contain it.](#)
190
191 [Authenticator Secret: The secret value contained within an authenticator.](#)

192 [Authenticity: The property that data originated from its purported source.](#)
193
194 [Bearer Assertion: An Assertion that does not provide a mechanism for the Subscriber to prove](#)
195 [that he or she is the rightful owner of the Assertion. The RP has to assume that the Assertion](#)
196 [was issued to the Subscriber who presents the Assertion or the corresponding Assertion](#)
197 [reference to the RP.](#)
198
199 [Bit: A binary digit: 0 or 1.](#)
200
201 [Biometrics: Automated recognition of individuals based on their behavioral and biological](#)
202 [characteristics. In this document, biometrics may be used to unlock authenticators and prevent](#)
203 [repudiation of Registration.](#)
204
205 [Certificate Authority \(CA\): A trusted entity that issues and revokes public key certificates.](#)
206
207 [Certificate Revocation List \(CRL\): A list of revoked public key certificates created and digitally](#)
208 [signed by a Certificate Authority. \[RFC 5280\]³](#)
209
210 [Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant](#)
211 [a challenge \(usually a random value or a nonce\) that the claimant combines with a secret \(such](#)
212 [as by hashing the challenge and a shared secret together, or by applying a private key operation](#)
213 [to the challenge\) to generate a response that is sent to the verifier. The verifier can](#)
214 [independently verify the response generated by the claimant \(such as by re-computing the hash](#)
215 [of the challenge and the shared secret and comparing to the response, or performing a public](#)
216 [key operation on the response\) and establish that the claimant possesses and controls the](#)
217 [secret.](#)
218
219 [Claimant: A Participant whose identity is to be verified using an authentication protocol.](#)
220 [Claimed Address: The physical location asserted by an individual \(e.g. an applicant\) where](#)
221 [he/she can be reached. It includes the residential street address of an individual and may also](#)
222 [include the mailing address of the individual. For example, a person with a foreign passport,](#)
223 [living in the U.S., will need to give an address when going through the Identity Proofing process.](#)
224 [This address would not be an “address of record” but a “claimed address.”](#)
225
226 [Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth](#)
227 [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>.

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>.

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

232
233 [Cookie: A character string, placed in a web browser's memory, which is available to websites](#)
234 [within the same Internet domain as the server that placed them in the web browser.](#)

235
236 [Credential: An object or data structure that authoritatively binds an identity \(and optionally,](#)
237 [additional attributes\) to an authenticator possessed and controlled by a Subscriber. While](#)
238 [common usage often assumes that the credential is maintained by the Subscriber, this](#)
239 [document also uses the term to refer to electronic records maintained by the CSP which](#)
240 [establish a binding between the Subscriber's authenticator\(s\) and identity.](#)

241
242 [Credential Service Provider \(CSP\): A trusted entity that issues or registers Subscriber](#)
243 [authenticators and issues electronic credentials to Subscribers. The CSP may encompass](#)
244 [Registration Authorities \(RAs\) and verifiers that it operates. A CSP may be an independent third](#)
245 [Participant, or may issue credentials for its own use.](#)

246
247 [Cross Site Request Forgery \(CSRF\): An attack in which a Subscriber who is currently](#)
248 [authenticated to an RP and connected through a secure session, browses to an attacker's](#)
249 [website which causes the Subscriber to unknowingly invoke unwanted actions at the RP. For](#)
250 [example, if a bank website is vulnerable to a CSRF attack, it may be possible for a Subscriber to](#)
251 [unintentionally authorize a large money transfer, merely by viewing a malicious link in a](#)
252 [webmail message while a connection to the bank is open in another browser window.](#)

253
254 [Cross Site Scripting \(XSS\): A vulnerability that allows attackers to inject malicious code into an](#)
255 [otherwise benign website. These scripts acquire the permissions of scripts generated by the](#)
256 [target website and can therefore compromise the confidentiality and integrity of data transfers](#)
257 [between the website and client. Websites are vulnerable if they display user supplied data from](#)
258 [requests or forms without sanitizing the data so that it is not executable.](#)

259
260 [Cryptographic Key: A value used to control cryptographic operations, such as decryption,](#)
261 [encryption, signature generation or signature verification. For the purposes of this document,](#)
262 [key requirements must meet the minimum requirements stated in Table 2 of NIST SP 800-57](#)
263 [Part 1. See also Asymmetric keys, Symmetric key.](#)

264
265 [Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.](#)

266
267 [Data Integrity: The property that data has not been altered by an unauthorized entity.](#)

268
269 [Derived Credential: A credential issued based on proof of possession and control of an](#)
270 [authenticator associated with a previously issued credential, so as not to duplicate the Identity](#)
271 [Proofing process.](#)

272
273 Digital Identity System: An Information System that supports Electronic Authentication and the
274 management of a person’s Identity in a digital environment. [Referenced in § 59.1-550, COV]
275
276 Digital Signature: An asymmetric key operation where the private key is used to digitally sign
277 data and the public key is used to verify the signature. Digital signatures provide authenticity
278 protection, integrity protection, and non-repudiation.
279
280 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication
281 protocol to capture information which can be used in a subsequent active attack to
282 masquerade as the claimant.
283
284 Electronic Authentication: The process of establishing confidence in user identities
285 electronically presented to an Information System.
286
287 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value
288 of a secret. Entropy is usually stated in bits.
289
290 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes
291 a class of data objects called XML documents and partially describes the behavior of computer
292 programs which process them.
293
294 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal
295 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI
296 Policy Authority to create, sign, and issue public key certificates to Principal CAs.
297
298 Federal Information Security Management Act (FISMA): Title III of the E-Government Act
299 requiring each federal agency to develop, document, and implement an agency-wide program
300 to provide information security for the information and Information Systems that support the
301 operations and assets of the agency, including those provided or managed by another agency,
302 contractor, or other source.
303
304 Federal Information Processing Standard (FIPS): Under the Information Technology
305 Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards
306 and guidelines that are developed by the National Institute of Standards and Technology (NIST)
307 for Federal computer systems. These standards and guidelines are issued by NIST as Federal
308 Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when
309 there are compelling Federal government requirements such as for security and interoperability
310 and there are no acceptable industry standards or solutions.⁵
311

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

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

315
316 Governance Authority: Entity responsible for providing policy level leadership, oversight,
317 strategic direction, and related governance activities within an Identity Trust Framework.

318
319 Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string.
320 Approved hash functions satisfy the following properties:

- 321 • (One-way) It is computationally infeasible to find any input that maps to any pre-
322 specified output, and
- 323 • (Collision resistant) It is computationally infeasible to find any two distinct inputs that
324 map to the same output.

325
326 Holder-of-Key Assertion: An Assertion that contains a reference to a symmetric key or a public
327 key (corresponding to a private key) held by the Subscriber. The RP may authenticate the
328 Subscriber by verifying that he or she can indeed prove possession and control of the
329 referenced key.

330
331 Identity: A set of attributes that uniquely describe a person within a given context.

332
333 Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's
334 claimed identity is their real identity.

335
336 Identity Proofing: The process by which a CSP and a Registration Authority (RA) collect and
337 verify information about a person for the purpose of issuing credentials to that person.

338
339 Identity Provider (IdP): The party that manages the subscriber's primary authentication
340 credentials and issues Assertions derived from those credentials generally to the credential
341 service provider (CSP).

342
343 Identity Trust Framework: A Digital Identity System with established identity, security, privacy,
344 technology, and enforcement rules and policies adhered to by certified identity providers that
345 are members of the Identity Trust Framework. Members of an Identity Trust Framework
346 include Identity Trust Framework operators and identity providers. Relying Participants may be,
347 but are not required to be, a member of an Identity Trust Framework in order to accept an
348 identity credential issued by a certified identity provider to verify an identity credential holder's
349 identity. [§ 59.1-550, COV]

350
351 Information System: A discrete set of information resources organized for the collection,
352 processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST
353 Interagency/Internal Report (IR) 7298 r. 2]

354

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

363
364 Knowledge Based Authentication: Authentication of an individual based on knowledge of
365 information associated with his or her claimed identity in public databases. Knowledge of such
366 information is considered to be private rather than secret, because it may be used in contexts
367 other than authentication to a verifier, thereby reducing the overall assurance associated with
368 the authentication process.

369
370 Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the
371 attacker positions himself or herself in between the claimant and verifier so that he can
372 intercept and alter data traveling between them.

373
374 Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric
375 key to detect both accidental and intentional modifications of the data. MACs provide
376 authenticity and integrity protection, but not non-repudiation protection.

377
378 Multi-Factor: A characteristic of an authentication system or an authenticator that uses more
379 than one authentication factor. The three types of authentication factors are something you
380 know, something you have, and something you are.

381
382 Network: An open communications medium, typically the Internet, that is used to transport
383 messages between the claimant and other Participants. Unless otherwise stated, no
384 assumptions are made about the security of the network; it is assumed to be open and subject
385 to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e.,
386 eavesdropping) attack at any point between the Participants (e.g., claimant, verifier, CSP or RP).

387
388 Nonce: A value used in security protocols that is never repeated with the same key. For
389 example, nonces used as challenges in challenge-response authentication protocols must not
390 be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay
391 attack. Using a nonce as a challenge is a different requirement than a random challenge,
392 because a nonce is not necessarily unpredictable.

393
394 Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on
395 an authentication protocol run or by penetrating a system and stealing security files) that
396 he/she is able to analyze in a system of his/her own choosing.

397

398 [Online Attack: An attack against an authentication protocol where the attacker either assumes](#)
399 [the role of a claimant with a genuine verifier or actively alters the authentication channel.](#)
400
401 [Online Guessing Attack: An attack in which an attacker performs repeated logon trials by](#)
402 [guessing possible values of the authenticator output.](#)
403
404 [Operational Authority: Entity responsible for operations, maintenance, management, and](#)
405 [related functions of an Identity Trust Framework.](#)
406
407 [Participant Requirements: A set of rules and policies in an Identity Trust Framework addressing](#)
408 [identity, security, privacy, technology, and enforcement, which are assigned to each member](#)
409 [type in a Digital Identity System. Member types include Registration Authorities \(RAs\), Identity](#)
410 [Providers \(IdPs\), Credential Service Providers \(CSPs\), Verifiers, and Relying Parties \(RPs\).](#)
411 [\[§ 59.1-550, COV\]](#)
412
413 [Passive Attack: An attack against an authentication protocol where the attacker intercepts data](#)
414 [traveling along the network between the claimant and verifier, but does not alter the data \(i.e.,](#)
415 [eavesdropping\).](#)
416
417 [Password: A secret that a claimant memorizes and uses to authenticate his or her identity.](#)
418 [Passwords are typically character strings.](#)
419
420 [Personal Identification Number \(PIN\): A password consisting only of decimal digits.](#)
421
422 [Personal Identity Verification \(PIV\) Card: Defined by \[FIPS 201\] as a physical artifact \(e.g.,](#)
423 [identity card, smart card\) issued to federal employees and contractors that contains stored](#)
424 [credentials \(e.g., photograph, cryptographic keys, digitized fingerprint representation\) so that](#)
425 [the claimed identity of the cardholder can be verified against the stored credentials by another](#)
426 [person \(human readable and verifiable\) or an automated process \(computer readable and](#)
427 [verifiable\).](#)
428
429 [Personally Identifiable Information \(PII\): As defined by OMB Circular A-130, Personally](#)
430 [Identifiable Information means information that can be used to distinguish or trace an](#)
431 [individual's identity, either alone or when combined with other information that is linked or](#)
432 [linkable to a specific individual.](#)
433
434 [Pharming: An attack in which an attacker corrupts an infrastructure service such as DNS](#)
435 [\(Domain Name Service\) causing the Subscriber to be misdirected to a forged verifier/RP, which](#)
436 [could cause the Subscriber to reveal sensitive information, download harmful software or](#)
437 [contribute to a fraudulent act.](#)
438 [Phishing: An attack in which the Subscriber is lured \(usually through an email\) to interact with a](#)
439 [counterfeit verifier/RP and tricked into revealing information that can be used to masquerade](#)
440 [as that Subscriber to the real verifier/RP.](#)
441

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

445

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

448

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

452

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

455

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

458

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

465

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

469

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

472

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

475

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

480

481 [Public Key Infrastructure \(PKI\): A set of policies, processes, server platforms, software and](#)
482 [workstations used for the purpose of administering certificates and public-private key pairs,](#)
483 [including the ability to issue, maintain, and revoke public key certificates.](#)

484

485 [Registration: The process through which an applicant applies to become a Subscriber of a CSP](#)
486 [and an RA validates the identity of the applicant on behalf of the CSP.](#)
487

488 [Registration Authority \(RA\): A trusted entity that establishes and vouches for the identity or](#)
489 [attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be](#)
490 [independent of a CSP, but it has a relationship to the CSP\(s\).](#)
491

492 [Relying Party \(RP\): An entity that relies upon the Subscriber's authenticator\(s\) and credentials](#)
493 [or a verifier's Assertion of a claimant's identity, typically to process a transaction or grant access](#)
494 [to information or a system.](#)
495

496 [Remote: \(As in remote authentication or remote transaction\) An information exchange](#)
497 [between network-connected devices where the information cannot be reliably protected end-](#)
498 [to-end by a single organization's security controls. Note: Any information exchange across the](#)
499 [Internet is considered remote.](#)
500

501 [Replay Attack: An attack in which the attacker is able to replay previously captured messages](#)
502 [\(between a legitimate claimant and a verifier\) to masquerade as that claimant to the verifier or](#)
503 [vice versa.](#)
504

505 [Risk Assessment: The process of identifying the risks to system security and determining the](#)
506 [probability of occurrence, the resulting impact, and additional safeguards that would mitigate](#)
507 [this impact. Part of Risk Management and synonymous with Risk Analysis.](#)
508

509 [Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the](#)
510 [results of computations for one instance cannot be reused by an attacker.](#)
511

512 [Secondary Authenticator: A temporary secret, issued by the verifier to a successfully](#)
513 [authenticated Subscriber as part of an Assertion protocol. This secret is subsequently used, by](#)
514 [the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer](#)
515 [Assertions, Assertion references, and Kerberos session keys.](#)
516

517 [Secure Sockets Layer \(SSL\): An authentication and security protocol widely implemented in](#)
518 [browsers and web servers. SSL has been superseded by the newer Transport Layer Security](#)
519 [\(TLS\) protocol; TLS 1.0 is effectively SSL version 3.1.](#)
520

521 [Security Assertion Mark-up Language \(SAML\): An XML-based security specification developed](#)
522 [by the Organization for the Advancement of Structured Information Standards \(OASIS\) for](#)
523 [exchanging authentication \(and authorization\) information between trusted entities over the](#)
524 [Internet.](#)
525 [SAML Authentication Assertion: A SAML Assertion that conveys information from a verifier to](#)
526 [an RP about a successful act of authentication that took place between the verifier and a](#)
527 [Subscriber.](#)
528

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

534

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

536

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

539

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

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

546

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

548

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

552

553 [Token: See Authenticator.](#)

554

555 [Token Authenticator: See Authenticator Output.](#)

556

557 [Token Secret: See Authenticator Secret.](#)

558

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

564

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

568

569 [Unverified Name: A Subscriber name that is not verified as meaningful by Identity Proofing.](#)

570

571 [Valid: In reference to an ID, the quality of not being expired or revoked.](#)

572

573 Verified Name: A Subscriber name that has been verified by Identity Proofing.
574
575 Verifier: An entity that verifies the claimant’s identity by verifying the claimant’s possession and
576 control of one or two authenticators using an authentication protocol. To do this, the verifier
577 may also need to validate credentials that link the authenticator(s) and identity and check their
578 status.
579
580 Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an
581 authentication protocol, usually to capture information that can be used to masquerade as a
582 claimant to the real verifier.
583
584 Virtual In-Person Proofing: A remote identity person proofing process that employs technical
585 and procedural measures that provide sufficient confidence that the remote session can be
586 considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]
587
588 Weakly Bound Credentials: Credentials that describe the binding between a user and
589 authenticator in a manner than can be modified without invalidating the credential.
590
591 Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero
592 so that the data is destroyed and not recoverable. This is often contrasted with deletion
593 methods that merely destroy reference to data within a file system rather than the data itself.
594
595 Zero-knowledge Password Protocol: A password based authentication protocol that allows a
596 claimant to authenticate to a Verifier without revealing the password to the verifier. Examples
597 of such protocols are EKE, SPEKE and SRP. Terms used in this document comply with definitions
598 in the Public Review version of the National Institute of Standards and Technology Special
599 Publication 800-63-3 (NIST SP 800-63-3), and align with adopted definitions in § 59.1-550, Code
600 of Virginia, and the Commonwealth of Virginia’s ITRM Glossary (ITRM Glossary):⁶
601
602 Active Attack: An online attack where the attacker transmits data to the claimant, credential
603 service provider, verifier, or relying party. Examples of active attacks include man-in-the-
604 middle, impersonation, and session hijacking.
605
606 Address of Record: The official location where an individual can be found. The address of record
607 always includes the residential street address of an individual and may also include the mailing
608 address of the individual. In very limited circumstances, an Army Post Office box number, Fleet
609 Post Office box number or the street address of next of kin or of another contact individual can
610 be used when a residential street address for the individual is not available.

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 HMSAC, 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

611
612 ~~Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An~~
613 ~~algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2)~~
614 ~~adopted in a FIPS or NIST Recommendation.~~

615
616 ~~Applicant: A party undergoing the processes of registration and identity proofing.~~

617
618 ~~Assertion: A statement from a verifier to a relying party (RP) that contains identity information~~
619 ~~about a subscriber. Assertions may also contain verified attributes.~~

620
621 ~~Assertion Reference: A data object, created in conjunction with an assertion, which identifies~~
622 ~~the verifier and includes a pointer to the full assertion held by the verifier.~~

623
624 ~~Assurance: In the context of [OMB M-04-04]⁷ and this document, assurance is defined as 1) the~~
625 ~~degree of confidence in the vetting process used to establish the identity of an individual to~~
626 ~~whom the credential was issued, and 2) the degree of confidence that the individual who uses~~
627 ~~the credential is the individual to whom the credential was issued.~~

628
629 ~~Asymmetric Keys: Two related keys, a public key and a private key that are used to perform~~
630 ~~complementary operations, such as encryption and decryption or signature generation and~~
631 ~~signature verification.~~

632
633 ~~Attack: An attempt by an unauthorized individual to fool a verifier or a relying party into~~
634 ~~believing that the unauthorized individual in question is the subscriber.~~

635
636 ~~Attacker: A party who acts with malicious intent to compromise an information system.~~

637
638 ~~Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or~~
639 ~~something.~~

640
641 ~~Authentication: The process of establishing confidence in the identity of users or information~~
642 ~~systems.~~

643
644 ~~Authentication Protocol: A defined sequence of messages between a claimant and a verifier~~
645 ~~that demonstrates that the claimant has possession and control of a valid authenticator to~~
646 ~~establish his/her identity, and optionally, demonstrates to the claimant that he or she is~~
647 ~~communicating with the intended verifier.~~

648
649 ~~Authentication Protocol Run: An exchange of messages between a claimant and a verifier that~~
650 ~~results in authentication (or authentication failure) between the two parties.~~

651

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

659
660 Authenticator: Something that the claimant possesses and controls (typically a cryptographic
661 module or password) that is used to authenticate the claimant's identity. In previous versions of
662 this guideline, this was referred to as a token.

663
664 Authenticator Assurance Level (AAL): A metric describing robustness of the authentication
665 process proving that the claimant is in control of a given subscriber's authenticator(s).

666
667 Authenticator Output: The output value generated by an authenticator. The ability to generate
668 valid authenticator outputs on demand proves that the claimant possesses and controls the
669 authenticator. Protocol messages sent to the verifier are dependent upon the authenticator
670 output, but they may or may not explicitly contain it.

671
672 Authenticator Secret: The secret value contained within an authenticator.

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

674
675 Bearer Assertion: An assertion that does not provide a mechanism for the subscriber to prove
676 that he or she is the rightful owner of the assertion. The RP has to assume that the assertion
677 was issued to the subscriber who presents the assertion or the corresponding assertion
678 reference to the RP.

679
680 Bit: A binary digit: 0 or 1.

681
682 Biometrics: Automated recognition of individuals based on their behavioral and biological
683 characteristics. In this document, biometrics may be used to unlock authenticators and prevent
684 repudiation of registration.

685
686 Certificate Authority (CA): A trusted entity that issues and revokes public key certificates.

687
688 Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally
689 signed by a Certificate Authority. [RFC 5280]⁸

690
691 Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant
692 a challenge (usually a random value or a nonce) that the claimant combines with a secret (such

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>.

693 as by hashing the challenge and a shared secret together, or by applying a private key operation
694 to the challenge) to generate a response that is sent to the verifier. The verifier can
695 independently verify the response generated by the claimant (such as by re-computing the hash
696 of the challenge and the shared secret and comparing to the response, or performing a public
697 key operation on the response) and establish that the claimant possesses and controls the
698 secret.

699
700 **Claimant:** A party whose identity is to be verified using an authentication protocol.

701
702 **Claimed Address:** The physical location asserted by an individual (e.g. an applicant) where
703 he/she can be reached. It includes the residential street address of an individual and may also
704 include the mailing address of the individual. For example, a person with a foreign passport,
705 living in the U.S., will need to give an address when going through the identity proofing process.
706 This address would not be an “address of record” but a “claimed address.”

707
708 **Claimed Identity:** A declaration by the applicant of their current Personal Name, date of birth
709 and address. [GPG45]⁹

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

714
715 **Cookie:** A character string, placed in a web browser’s memory, which is available to websites
716 within the same Internet domain as the server that placed them in the web browser.

717
718 **Credential:** An object or data structure that authoritatively binds an identity (and optionally,
719 additional attributes) to an authenticator possessed and controlled by a subscriber. While
720 common usage often assumes that the credential is maintained by the subscriber, this
721 document also uses the term to refer to electronic records maintained by the CSP which
722 establish a binding between the subscriber’s authenticator(s) and identity.

723
724 **Credential Service Provider (CSP):** A trusted entity that issues or registers subscriber
725 authenticators and issues electronic credentials to subscribers. The CSP may encompass
726 Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third
727 party, or may issue credentials for its own use.

728
729 **Cross Site Request Forgery (CSRF):** An attack in which a subscriber who is currently
730 authenticated to an RP and connected through a secure session, browses to an attacker’s
731 website which causes the subscriber to unknowingly invoke unwanted actions at the RP. For

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>.

732 example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to
733 unintentionally authorize a large money transfer, merely by viewing a malicious link in a
734 webmail message while a connection to the bank is open in another browser window.
735

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

742 Cryptographic Key: A value used to control cryptographic operations, such as decryption,
743 encryption, signature generation or signature verification. For the purposes of this document,
744 key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57
745 Part 1. See also Asymmetric keys, Symmetric key.
746

747 Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.
748

749 Data Integrity: The property that data has not been altered by an unauthorized entity.
750

751 Derived Credential: A credential issued based on proof of possession and control of an
752 authenticator associated with a previously issued credential, so as not to duplicate the identity
753 proofing process.
754

755 Digital Signature: An asymmetric key operation where the private key is used to digitally sign
756 data and the public key is used to verify the signature. Digital signatures provide authenticity
757 protection, integrity protection, and non-repudiation.
758

759 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication
760 protocol to capture information which can be used in a subsequent active attack to
761 masquerade as the claimant.
762

763 Electronic Authentication: The process of establishing confidence in user identities
764 electronically presented to an information system.
765

766 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value
767 of a secret. Entropy is usually stated in bits.
768

769 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes
770 a class of data objects called XML documents and partially describes the behavior of computer
771 programs which process them.
772

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

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

781
782 Federal Information Processing Standard (FIPS): Under the Information Technology
783 Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards
784 and guidelines that are developed by the National Institute of Standards and Technology (NIST)
785 for Federal computer systems. These standards and guidelines are issued by NIST as Federal
786 Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when
787 there are compelling Federal government requirements such as for security and interoperability
788 and there are no acceptable industry standards or solutions.⁴⁰

789
790 Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string.
791 Approved hash functions satisfy the following properties:

- 792 • (One-way) It is computationally infeasible to find any input that maps to any pre-
793 specified output, and
- 794 • (Collision resistant) It is computationally infeasible to find any two distinct inputs that
795 map to the same output.

796 Holder of Key Assertion: An assertion that contains a reference to a symmetric key or a public
797 key (corresponding to a private key) held by the subscriber. The RP may authenticate the
798 subscriber by verifying that he or she can indeed prove possession and control of the
799 referenced key.

800
801 Identity: A set of attributes that uniquely describe a person within a given context.

802
803 Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's
804 claimed identity is their real identity.

805
806 Identity Proofing: The process by which a CSP and a Registration Authority (RA) collect and
807 verify information about a person for the purpose of issuing credentials to that person.

808
809 Kerberos: A widely used authentication protocol developed at MIT. In "classic" Kerberos, users
810 share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to
811 communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by
812 the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords,
813 the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who
814 capture the initial user-to-KDC exchange. Longer password length and complexity provide
815 some mitigation to this vulnerability, although sufficiently long passwords tend to be
816 cumbersome for users.

817

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

818 ~~Knowledge Based Authentication: Authentication of an individual based on knowledge of~~
819 ~~information associated with his or her claimed identity in public databases. Knowledge of such~~
820 ~~information is considered to be private rather than secret, because it may be used in contexts~~
821 ~~other than authentication to a verifier, thereby reducing the overall assurance associated with~~
822 ~~the authentication process.~~

823
824 ~~Man in the Middle Attack (MitM): An attack on the authentication protocol run in which the~~
825 ~~attacker positions himself or herself in between the claimant and verifier so that he can~~
826 ~~intercept and alter data traveling between them.~~

827
828 ~~Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric~~
829 ~~key to detect both accidental and intentional modifications of the data. MACs provide~~
830 ~~authenticity and integrity protection, but not non-repudiation protection.~~

831
832 ~~Multi-Factor: A characteristic of an authentication system or an authenticator that uses more~~
833 ~~than one authentication factor. The three types of authentication factors are something you~~
834 ~~know, something you have, and something you are.~~

835
836

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

842
843 ~~Nonce: A value used in security protocols that is never repeated with the same key. For~~
844 ~~example, nonces used as challenges in challenge-response authentication protocols must not~~
845 ~~be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay~~
846 ~~attack. Using a nonce as a challenge is a different requirement than a random challenge,~~
847 ~~because a nonce is not necessarily unpredictable.~~

848
849 ~~Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on~~
850 ~~an authentication protocol run or by penetrating a system and stealing security files) that~~
851 ~~he/she is able to analyze in a system of his/her own choosing.~~

852
853 ~~Online Attack: An attack against an authentication protocol where the attacker either assumes~~
854 ~~the role of a claimant with a genuine verifier or actively alters the authentication channel.~~

855
856 ~~Online Guessing Attack: An attack in which an attacker performs repeated logon trials by~~
857 ~~guessing possible values of the authenticator output.~~

858
859 ~~Passive Attack: An attack against an authentication protocol where the attacker intercepts data~~
860 ~~traveling along the network between the claimant and verifier, but does not alter the data (i.e.,~~
861 ~~eavesdropping).~~

862
863 ~~Password: A secret that a claimant memorizes and uses to authenticate his or her identity.~~
864 ~~Passwords are typically character strings.~~

865
866 ~~Personal Identification Number (PIN): A password consisting only of decimal digits.~~

867
868 ~~Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,~~
869 ~~identity card, smart card) issued to federal employees and contractors that contains stored~~
870 ~~credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that~~
871 ~~the claimed identity of the cardholder can be verified against the stored credentials by another~~
872 ~~person (human readable and verifiable) or an automated process (computer readable and~~
873 ~~verifiable).~~

874
875 ~~Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally~~
876 ~~Identifiable Information means information that can be used to distinguish or trace an~~
877 ~~individual's identity, either alone or when combined with other information that is linked or~~
878 ~~linkable to a specific individual.~~

879

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

884

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

888

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

891

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

895

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

898

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

901

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

908

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

912

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

915

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

918

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

923

924 ~~Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and~~
925 ~~workstations used for the purpose of administering certificates and public-private key pairs,~~
926 ~~including the ability to issue, maintain, and revoke public key certificates.~~
927
928 ~~Registration: The process through which an applicant applies to become a subscriber of a CSP~~
929 ~~and an RA validates the identity of the applicant on behalf of the CSP.~~
930
931 ~~Registration Authority (RA): A trusted entity that establishes and vouches for the identity or~~
932 ~~attributes of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be~~
933 ~~independent of a CSP, but it has a relationship to the CSP(s).~~
934
935 ~~Relying Party (RP): An entity that relies upon the subscriber's authenticator(s) and credentials~~
936 ~~or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access~~
937 ~~to information or a system.~~
938
939 ~~Remote: (As in remote authentication or remote transaction) An information exchange~~
940 ~~between network-connected devices where the information cannot be reliably protected end-~~
941 ~~to-end by a single organization's security controls. Note: Any information exchange across the~~
942 ~~Internet is considered remote.~~
943
944 ~~Replay Attack: An attack in which the attacker is able to replay previously captured messages~~
945 ~~(between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or~~
946 ~~vice-versa.~~
947
948 ~~Risk Assessment: The process of identifying the risks to system security and determining the~~
949 ~~probability of occurrence, the resulting impact, and additional safeguards that would mitigate~~
950 ~~this impact. Part of Risk Management and synonymous with Risk Analysis.~~
951
952 ~~Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the~~
953 ~~results of computations for one instance cannot be reused by an attacker.~~
954
955 ~~Secondary Authenticator: A temporary secret, issued by the verifier to a successfully~~
956 ~~authenticated subscriber as part of an assertion protocol. This secret is subsequently used, by~~
957 ~~the subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer~~
958 ~~assertions, assertion references, and Kerberos session keys.~~
959
960 ~~Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in~~
961 ~~browsers and web servers. SSL has been superseded by the newer Transport Layer Security~~
962 ~~(TLS) protocol; TLS 1.0 is effectively SSL version 3.1.~~
963
964 ~~Security Assertion Mark up Language (SAML): An XML-based security specification developed~~
965 ~~by the Organization for the Advancement of Structured Information Standards (OASIS) for~~
966 ~~exchanging authentication (and authorization) information between trusted entities over the~~
967 ~~Internet.~~

968 ~~SAML Authentication Assertion: A SAML assertion that conveys information from a verifier to~~
969 ~~an RP about a successful act of authentication that took place between the verifier and a~~
970 ~~subscriber.~~

971

972 ~~Session Hijack Attack: An attack in which the attacker is able to insert himself or herself~~
973 ~~between a claimant and a verifier subsequent to a successful authentication exchange between~~
974 ~~the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to~~
975 ~~control session data exchange. Sessions between the claimant and the relying party can also be~~
976 ~~similarly compromised.~~

977

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

979

980 ~~Social Engineering: The act of deceiving an individual into revealing sensitive information by~~
981 ~~associating with the individual to gain confidence and trust.~~

982

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

987

988 ~~Strongly Bound Credentials: Credentials that describe the binding between a user and~~
989 ~~authenticator in a tamper-evident fashion.~~

990

991 ~~Subscriber: A party who has received a credential or authenticator from a CSP.~~

992

993 ~~Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation~~
994 ~~and its inverse, for example to encrypt and decrypt, or create a message authentication code~~
995 ~~and to verify the code.~~

996

997 ~~Token: See Authenticator.~~

998

999 ~~Token Authenticator: See Authenticator Output.~~

1000

1001 ~~Token Secret: See Authenticator Secret.~~

1002

1003 ~~Transport Layer Security (TLS): An authentication and security protocol widely implemented in~~
1004 ~~browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure~~
1005 ~~Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52,~~
1006 ~~Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies~~
1007 ~~how TLS is to be used in government applications.~~

1008

1009 ~~Trust Anchor: A public or symmetric key that is trusted because it is directly built into hardware~~
1010 ~~or software, or securely provisioned via out-of-band means, rather than because it is vouched~~
1011 ~~for by another trusted entity (e.g. in a public key certificate).~~

1012 ~~Trust Framework: In identity management, means a digital identity system with established~~
1013 ~~identity, security, privacy, technology, and enforcement rules and policies adhered to by~~
1014 ~~certified identity providers that are members of the identity trust framework. Members of an~~
1015 ~~identity trust framework include identity trust framework operators and identity providers.~~
1016 ~~Relying parties may be, but are not required to be, a member of an identity trust framework in~~
1017 ~~order to accept an identity credential issued by a certified identity provider to verify an identity~~
1018 ~~credential holder's identity. [§ 59.1-550, Code of Virginia]~~
1019
1020 ~~Unverified Name: A subscriber name that is not verified as meaningful by identity proofing.~~
1021
1022 ~~Valid: In reference to an ID, the quality of not being expired or revoked.~~
1023
1024 ~~Verified Name: A subscriber name that has been verified by identity proofing.~~
1025
1026 ~~Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and~~
1027 ~~control of one or two authenticators using an authentication protocol. To do this, the verifier~~
1028 ~~may also need to validate credentials that link the authenticator(s) and identity and check their~~
1029 ~~status.~~
1030
1031 ~~Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an~~
1032 ~~authentication protocol, usually to capture information that can be used to masquerade as a~~
1033 ~~claimant to the real verifier.~~
1034
1035 ~~Weakly Bound Credentials: Credentials that describe the binding between a user and~~
1036 ~~authenticator in a manner that can be modified without invalidating the credential.~~
1037
1038 ~~Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero~~
1039 ~~so that the data is destroyed and not recoverable. This is often contrasted with deletion~~
1040 ~~methods that merely destroy reference to data within a file system rather than the data itself.~~
1041
1042 ~~Zero-knowledge Password Protocol: A password-based authentication protocol that allows a~~
1043 ~~claimant to authenticate to a Verifier without revealing the password to the verifier. Examples~~
1044 ~~of such protocols are EKE, SPEKE and SRP.~~

1045 5 Background

1046
1047 In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter
1048 ~~50 of Title 59.1, Code of Virginia~~) to address demand in the state’s digital economy for secure,
1049 privacy enhancing ~~electronic authentication~~Electronic Authentication and identity
1050 management. Growing numbers of “communities of interest” have advocated for stronger,
1051 scalable and interoperable identity solutions to increase consumer protection and reduce
1052 liability for principal actors in the identity ecosystem – Identity Providers, Credential Service
1053 Providers and Relying Parties.

1054
1055 ~~To address the demand contemplated by the Electronic Identity Management Act, the General~~
1056 ~~Assembly also created the Identity Management Standards Advisory Council (IMSAC) to advise~~
1057 ~~the Secretary of Technology on the adoption of identity management standards and the~~
1058 ~~creation of guidance documents, pursuant to §2.2-436. A copy of the IMSAC Charter has been~~
1059 ~~provided in Appendix 1. The following guidance document has been developed by the Virginia~~
1060 ~~Information Technologies Agency (VITA), acting on behalf of the Secretary of Technology and~~
1061 ~~Chief Information Officer of the Commonwealth, at the direction of IMSAC. IMSAC was created~~
1062 ~~by the General Assembly as part of the Act and advises the Secretary of Technology on the~~
1063 ~~adoption of identity management standards and the creation of guidance documents pursuant~~
1064 ~~to §2.2-436. A copy of the IMSAC Charter has been provided in Appendix 1.~~

1065
1066 The Advisory Council recommends to the Secretary of Technology guidance documents relating
1067 to (i) nationally recognized technical and data standards regarding the verification and
1068 authentication of identity in digital and online transactions; (ii) the minimum specifications and
1069 standards that should be included in an ~~identity~~Identity Trust Framework, as defined in §59.1-
1070 550, so as to warrant liability protection pursuant to the Electronic Identity Management Act
1071 (§59.1-550 et seq.); and (iii) any other related data standards or specifications concerning
1072 reliance by third parties on identity credentials, as defined in §59.1-550.

1074 Purpose Statement

1075
1076 ~~On behalf of the Secretary of Technology, and acting at the direction of IMSAC, this guidance~~
1077 ~~document has been developed by the Virginia Information Technologies Agency (VITA). The~~
1078 ~~purpose of this document is to establish minimum specifications for~~ ~~electronic-Assertions~~
1079 ~~authentication within an identity management system a Digital Identity System. The document~~
1080 ~~assumes that the identity management system will be supported by a trust framework,~~
1081 ~~compliant with Applicable Law.⁴⁴ The minimum specifications have been stated based on~~
1082 ~~language in~~ ~~designed to be conformant with~~ NIST SP 800-63C-3.
1083

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.~~

1084 The document defines ~~minimum requirements~~ Assertion types, core components, presentation
1085 ~~methods, security, and process flows, assurance levels and~~ privacy and security provisions for
1086 ~~Assertions for electronic authentication~~. The document assumes that specific business, legal,
1087 and technical requirements for ~~electronic authentication~~ Assertions will be established in the
1088 ~~Trust Framework~~ Identity Trust Framework for each distinct ~~identity management system~~ Digital
1089 Identity System, and that these requirements will be designed based on the Electronic
1090 Authentication model, Identity Assurance Level (IAL), and Authenticator Assurance Level (AAL)
1091 requirements for the system.

1092
1093 The document limits its focus to ~~electronic authentication~~ Assertions. Minimum specifications
1094 for other components of ~~an identity management system~~ a Digital Identity System will have
1095 been defined in separate IMSAC guidance documents in this series, pursuant to §2.2-436 and
1096 §2.2-437.

1097

1098 6 Minimum Specifications

1099

1100 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3)
1101 defines an “~~electronic authentication~~ Assertion” in a Digital Identity System as “A statement
1102 from a verifier to a relying party (RP) that contains identity information about a Subscriber.
1103 ~~Assertions may also contain verified attributes~~ the process of establishing confidence in the
1104 ~~identity of users or information systems~~.”¹² Information systems may use the
1105 authenticated identity to determine if that user is authorized to perform an electronic
1106 transaction.

1107

1108 This document establishes minimum specifications for ~~electronic authentication~~ Assertions
1109 within a Digital Identity System conformant with, and using language from, NIST SP 800-63-3.
1110 However, the minimum specifications defined in this document have been developed to
1111 accommodate requirements for ~~electronic authentication~~ Assertions established under other
1112 national and international standards.¹³ The minimum specifications in this document also
1113 assume that specific business, legal, and technical requirements for ~~an identity management~~
1114 ~~system~~ a Digital Identity System will be documented in the ~~trust framework~~ Identity Trust
1115 Framework for that system. Minimum specifications for other components of ~~an identity~~
1116 ~~management system~~ a Digital Identity System have been documented in separate guidance
1117 documents in the IMSAC series, pursuant to §2.2-436 and §2.2-437.

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.

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>.

1118
 1119
 1120
 1121
 1122
 1123
 1124
 1125
 1126
 1127
 1128
 1129
 1130
 1131
 1132
 1133
 1134
 1135
 1136
 1137
 1138

Electronic Authentication Model

~~Assertions play an integral role in~~ Electronic ~~authentication~~ Authentication, is the process of establishing confidence in individual identities presented to a ~~digital system~~ Digital Identity System. ~~Digital Identity Systems can use~~ Digital Identity Systems ~~can use~~ implement Assertions as part of the process to ~~authenticate a person's Identity. In turn,~~ the authenticated identity ~~to may be used to~~ determine if that ~~individual person~~ individual person is authorized to perform an online transaction. The minimum specifications in this document assume that the authentication and transaction take place across a network.

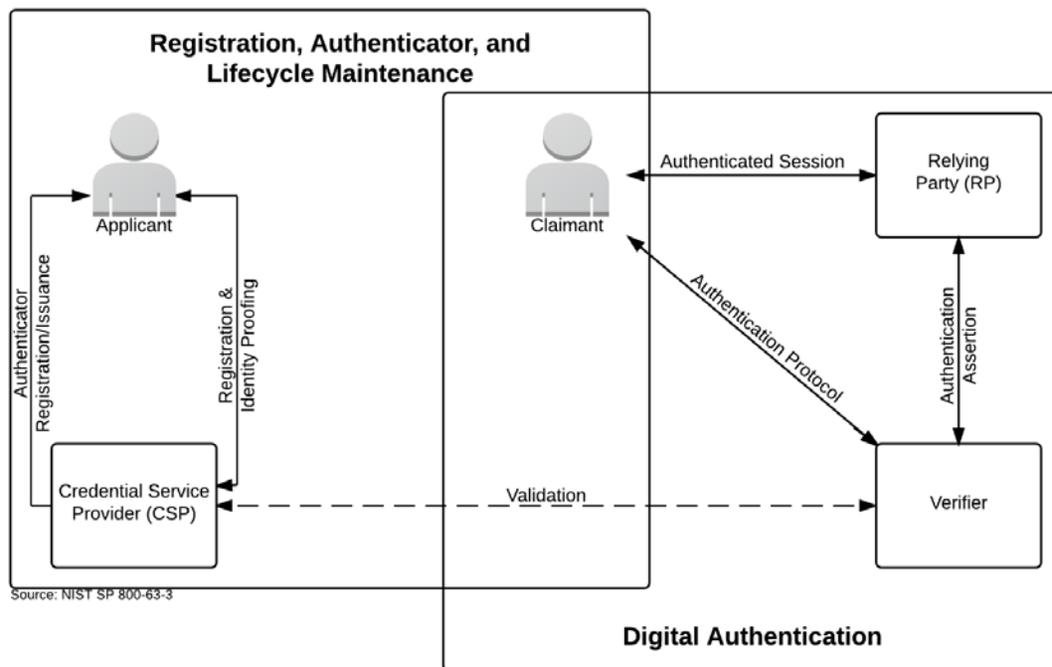
~~The electronic authentication model~~ The minimum specifications for Assertions defined in this document reflect the Electronic Authentication model defined in these minimum specifications ~~reflects current technologies and architectures~~ used primarily by governmental entities. More complex models that separate functions among a broader range of parties are also available and may have advantages in some classes of applications. While a simpler model ~~has been defined in~~ serves as the basis for these minimum specifications, it does not preclude ~~participant members~~ in identity management system Digital Identity Systems from separating these functions. ~~Minimum specifications for the Electronic Authentication model reflected in this document have been defined in ITRM Guidance Document: Electronic Authentication, and a graphic of the model has been shown in Figure 1.~~

Formatted: Font: Italic

Formatted: Font: Bold

1139

Figure 1. Electronic Authentication Model



1140
1141
1142
1143
1144
1145
1146

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: Width: 11", Height: 8.5"

Formatted: Centered

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

1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189

Assertions

An Assertion contains a set of claims or statements about an authenticated Subscriber. Assertions can be categorized along multiple orthogonal dimensions, including the characteristics of using the Assertion or the protections on the Assertion itself.

The core set of claims inside an Assertion should include (but may not be limited to):

- Issuer: Identifier for the party that issued the Assertion (usually the IdP)
- Subject: Identifier for the party that the Assertion is about (the Subscriber), usually within the namespace control of the issuer (IdP)
- Audience: Identifier for the party intended to consume the Assertion, primarily the RP
- Issuance: Timestamp indicating when the Assertion was issued by the IdP
- Expiration: Timestamp indicating when the Assertion expires and will no longer be accepted as valid by the RP (Note: This is not the expiration of the session at the RP)
- Authentication Time: Timestamp indicating when the IdP last verified the presence of the Subscriber at the IdP through a primary Authentication event
- Identifier: Random value uniquely identifying this Assertion, used to prevent attackers from manufacturing malicious Assertions which would pass other validity checks

These core claims, particularly the issuance and expiration claims, apply to the Assertion about the Authentication event itself, and not to any additional Identity Attributes associated with the Subscriber, even when those claims are included within the Assertion. A Subscriber's Attributes may expire or be otherwise invalidated independently of the expiration or invalidation of the Assertion.

Assertions may include other additional Identity Attributes. Privacy requirements for presenting Attributes in Assertions have been provided below in this document. The RP may fetch additional Identity Attributes from the IdP in a separate transaction using an authorization Credential issued alongside the Assertion.

Although details vary based on the exact Authentication or federation protocols in use, an Assertion should be used only to represent a single log-in event at the RP. After the RP consumes the Assertion, session management at the RP comes into play and the Assertion is no longer used directly. The expiration of the Assertion must not represent the expiration of the session at the RP.

Assertion Possession Category

An Assertion can be classified based on whether possession of the Assertion itself is sufficient for representing the subject of the Assertion, or if additional proof is necessary alongside the Assertion.

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

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

1190
1191
1192 Holder-of-Key Assertions
1193 A Holder-of-Key Assertion contains a reference to a Symmetric Key or a Public Key
1194 (corresponding to a Private Key) possessed by and representing the Subscriber. An RP may
1195 decide when to require the Subscriber to prove possession of the key, depending on the policy
1196 of the RP. However, the RP must require the Subscriber to prove possession of the key that is
1197 referenced in the Assertion in parallel with presentation of the Assertion itself in order for the
1198 Assertion to be considered Holder-Of-Key. Otherwise, an Assertion containing reference to a
1199 key which the user has not proved possession of will be considered a Bearer Assertion.

1200
1201 The key referenced in a Holder-of-Key represents the Subscriber, not the client. This key may be
1202 distinct from any key used by the Subscriber to Authenticate to the IdP. In proving possession
1203 of the Subscriber's secret, the Subscriber also proves with a certain degree of assurance that
1204 they are the rightful subject of the Assertion. It is more difficult for an attacker to use a stolen
1205 Holder-of-Key Assertion issued to a Subscriber, since the attacker would need to steal the
1206 referenced key material as well.

1207
1208 Note that the reference to the key material in question is asserted by the issuer of the Assertion
1209 as are any other claims therein, and reference to a given key must be trusted at the same level
1210 as all other claims within the Assertion itself. The Assertion must not include an unencrypted
1211 Private or Symmetric Key to be used with Holder-of-Key presentation.

1212
1213 Bearer Assertions
1214 A bearer Assertion can be presented by any party as proof of the bearer's identity, without
1215 reference to external materials. If an attacker is able to capture or manufacture a valid
1216 Assertion representing a Subscriber, and that attacker is able to successfully present that
1217 Assertion to the RP, then the attacker will be able to impersonate the Subscriber at that RP.

1218
1219 Note that mere possession of a bearer Assertion is not always enough to impersonate a
1220 Subscriber. For example, if an Assertion is presented in the indirect federation model (Section
1221 6.1), additional controls may be placed on the transaction (such as identification of the RP and
1222 Assertion injection protections) that help to further protect the RP from fraudulent activity.

1223
1224 Assertion Protection Category

1225
1226 Regardless of the possession mechanism used to obtain them, Assertions must include an
1227 appropriate set of protections to the Assertion data itself to prevent attackers from
1228 manufacturing valid Assertions or re-using captured Assertions at disparate RPs.

1229
1230 Assertion Identifier
1231 Assertions must contain sufficient Entropy to prevent an attacker from manufacturing a valid
1232 Assertion and using it with a target RP. Assertions may accomplish this by use of an embedded
1233 Nonce, timestamp, Assertion identifier, or a combination of these or other techniques. In the

Formatted: Font: 13 pt

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

1234 [absence of additional Cryptographic protections, this source of randomness must function as a](#)
1235 [shared secret between the IdP and the RP to uniquely identify the Assertion in question.](#)
1236 [Signed Assertion](#)
1237 [Assertions may be Cryptographically signed by the IdP, and the RP must validate the signature](#)
1238 [of each such Assertion based on the IdP's key. This signature must cover all vital fields of the](#)
1239 [Assertion, including its issuer, audience, subject, expiration, and any unique identifiers.](#)
1240
1241 [The signature may be asymmetric based on the published Public Key of the IdP. In such cases,](#)
1242 [the RP may fetch this Public Key in a secure fashion at runtime \(such as through an HTTPS URL](#)
1243 [hosted by the IdP\), or the key may be provisioned out of band at the RP \(during configuration of](#)
1244 [the RP\). The signature may be symmetric based on a key shared out of band between the IdP](#)
1245 [and the RP. In such circumstances, the IdP must use a different shared key for each RP. All](#)
1246 [signatures must use approved signing methods.](#)
1247
1248 [Encrypted Assertion](#)
1249 [Assertions may be encrypted in such a fashion as to allow only the intended audience to](#)
1250 [decrypt the claims therein. The IdP must encrypt the payload of the Assertion using the RP's](#)
1251 [Public Key. The IdP may fetch this Public Key in a secure fashion at runtime \(such as through an](#)
1252 [HTTPS URL hosted by the RP\), or the key may be provisioned out of band at the IdP \(during](#)
1253 [registration of the RP\). All encrypted objects must use approved encryption methods.](#)
1254
1255 [Audience Restriction](#)
1256 [All Assertions should use audience restriction techniques to allow an RP to recognize whether](#)
1257 [or not it is the intended target of an issued Assertion. All RPs must check the audience of an](#)
1258 [Assertion, if provided, to prevent the injection and replay of an Assertion generated for one RP](#)
1259 [at another RP.](#)
1260
1261 [Pairwise Pseudonymous Identifiers](#)
1262 [In some circumstances, it is desirable to prevent the Subscriber's account at the IdP from being](#)
1263 [linked through one or more RPs through use of a common identifier. In these circumstances,](#)
1264 [pairwise Pseudonymous Identifiers must be used within the Assertions generated by the IdP for](#)
1265 [the RP, and the IdP must generate a different identifier for each RP. \(See Pairwise](#)
1266 [Pseudonymous Identifier Generation for more information.\)](#)
1267
1268 [When unique Pseudonymous Identifiers are used with RPs alongside of Identity Attribute](#)
1269 [bundles, it may still be possible for multiple colluding RPs to fully identify and correlate a](#)
1270 [Subscriber across Digital Identity Systems using these attributes. For example, given that two](#)
1271 [independent RPs will each see the same Subscriber identified with a different pairwise](#)
1272 [Pseudonymous Identifier, the RPs could still determine that the Subscriber is the same person](#)
1273 [by comparing their name, email address, Physical Address, or other identifying Attributes](#)
1274 [carried alongside the pairwise Pseudonymous Identifier. Privacy policies may prohibit such](#)
1275 [correlation, but pairwise Pseudonymous Identifiers can increase effectiveness of these policies](#)
1276 [by increasing the administrative effort in managing the Attribute correlation.](#)
1277

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

1278
1279 Note that in a proxied federation model, ultimate IdP may be unable to generate a pairwise
1280 Pseudonymous Identifier for the ultimate RP, since the proxy could blind the IdP from knowing
1281 which RP is being accessed by the Subscriber. In such situations, the pairwise Pseudonymous
1282 Identifier is usually between the IdP and the federation proxy itself. The proxy, acting as an IdP,
1283 can itself provide pairwise Pseudonymous Identifiers to downstream RPs. Depending on the
1284 protocol, the federation proxy may need to map the pairwise Pseudonymous Identifiers back to
1285 the associated identifiers from upstream IdPs in order to allow the Identity protocol to function.
1286 In such cases, the proxy will be able to track and determine which pairwise Pseudonymous
1287 Identifiers represent the same Subscriber at different RPs.

1288 Pairwise Pseudonymous Identifier Generation

1289 Pairwise Pseudonymous Identifiers must be opaque and unguessable, containing no identifying
1290 information about the Subscriber. Additionally, the identifiers must only be known by and used
1291 by one IdP-RP pair. An IdP may generate the same identifier for a Subscriber at multiple RPs at
1292 the request of those RPs, but only if:

- 1293 • Those RPs have a demonstrable relationship that justifies an operational need for the
- 1294 correlation, such as a shared security domain or shared legal ownership, and
- 1295 • All RPs sharing an identifier consent to being correlated in such a manner.

1296 The RPs must conduct a privacy risk assessment to consider the privacy risks associated with
1297 requesting a common identifier. The IdP must ensure that only intended RPs are correlated;
1298 otherwise, a rogue RP could learn of the Pseudonymous Identifier for a correlation by
1299 fraudulently posing as part of that correlation.

1300 Assertion Presentation

1301 Assertions may be presented in either a back-channel or front-channel manner from the IdP to
1302 the RP. Each model has its benefits and drawbacks, but both require the proper validation of
1303 the Assertion. Assertions may also be proxied to facilitate federation between IdPs and RPs
1304 under specific circumstances. The IdP must transmit only those Attributes that were explicitly
1305 requested by the RP. RPs must conduct a privacy risk assessment when determining which
1306 attributes to request.

1307 The Subscriber must be able to view the Attribute values to be transmitted, although masking
1308 mechanisms must be employed, as necessary, to mitigate the risk of unauthorized exposure of
1309 sensitive information (e.g. shoulder surfing). The Subscriber must receive explicit notice and be
1310 able to provide positive confirmation before any attributes about the Subscriber are
1311 transmitted to any RP.

1312 At a minimum, the notice should be provided by the party in the position to provide the most
1313 effective notice and obtain confirmation. If the protocol in use allows for optional Attributes,
1314 the Subscriber must be given the option to decide whether to transmit those Attributes to the
1315 RP.

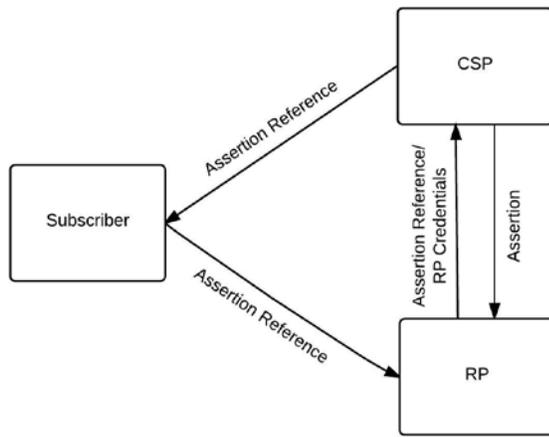
Formatted: List Paragraph, Bulleted + Level: 1
+ Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: 13 pt

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

1321 RP. A IdP may employ mechanisms to remember and re-transmit the exact Attribute bundle to
 1322 the same RP.
 1323 Back-Channel Presentation
 1324 In the back-channel model, the Subscriber is given an Assertion reference to present to the RP,
 1325 generally through the front channel. The Assertion reference itself contains no information
 1326 about the Subscriber and must be resistant to tampering and fabrication by an attacker. The RP
 1327 presents the Assertion reference to the IdP, usually along with authentication of the RP itself, to
 1328 fetch the Assertion. Figure 2 shows the back-channel presentation model.

1330 Figure 2. Back-Channel Assertion Presentation



Source: NIST SP 800-63C

1331
 1332
 1333 In the back-channel model, the Assertion itself is requested directly from the IdP to the RP,
 1334 minimizing chances of interception and manipulation by a third party (including the Subscriber
 1335 themselves). This method also allows the RP to query the CSP for additional attributes about
 1336 the Subscriber not included in the Assertion itself, since back-channel communication can
 1337 continue to occur after the initial authentication transaction has completed.

1338
 1339 The back-channel method also requires more network transactions than the front-channel
 1340 model, but the information is limited to the only required parties. Since an RP is expecting to
 1341 get an Assertion only from the IdP directly, the attack surface is reduced since it is more difficult
 1342 to inject Assertions directly into the RP.

1343 The Assertion Reference:

- 1345 • Must be limited to use by a single RP
- 1346 • Must be single-use
- 1347 • Should be time limited with a short lifetime of seconds or minutes

- Formatted: Font: Bold
- Formatted: Centered

- Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"
- Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1348 • Should be presented along with authentication of the RP
 1349 The RP must protect itself against injection of manufactured or captured Assertion references
 1350 by use of cross-site scripting protection or other accepted techniques. Claims within the
 1351 Assertion must be validated including issuer verification, signature validation, and audience
 1352 restriction.

1353
 1354 Conveyance of the Assertion reference from the IdP to the Subscriber as well as from the
 1355 Subscriber to the RP must be made over an authenticated protected channel. Conveyance of
 1356 the Assertion reference from the RP to the IdP as well as the Assertion from the IdP to the RP
 1357 must be made over an authenticated protected channel. Presentation of the Assertion
 1358 reference at the IdP should require Authentication of the RP before issuance of an Assertion.

1359 Front-Channel Presentation

1361 In the front-channel model, the IdP creates an Assertion and sends it to the Subscriber after
 1362 successful Authentication. The Assertion is used by the Subscriber to authenticate to the RP.
 1363 This is often handled by mechanisms within the Subscriber’s browser. **Figure 3** shows the front-
 1364 channel presentation model.

Formatted: Font: Bold

1365 **Figure 3: Front-Channel Assertion Presentation**

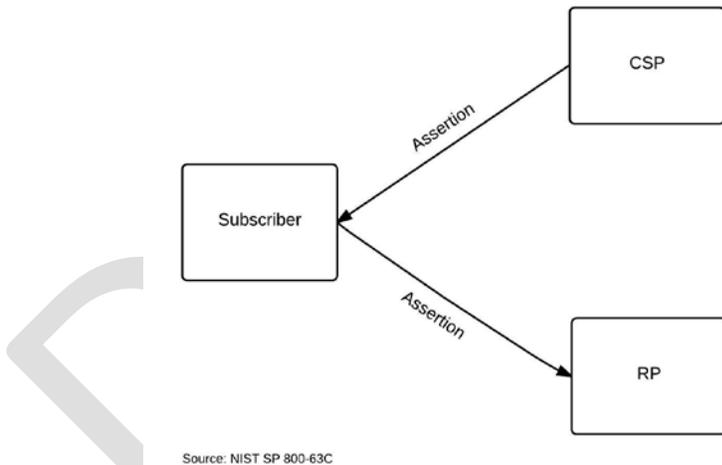
Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Centered



Formatted: Font: Bold

1367
 1368 In the front-channel method, an Assertion is visible to the Subscriber, which could potentially
 1369 cause leakage of system information included in the Assertion. Since the Assertion is under the
 1370 control of the Subscriber, the front-channel presentation method also allows the Subscriber to
 1371 submit a single Assertion to unintended parties, perhaps by a browser replaying an Assertion at
 1372 multiple RPs. Even if the Assertion is audience restricted and rejected by RPs, its presentation at
 1373

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

1374 unintended RPs could lead to leaking information about the Subscriber and their online
 1375 activities.

1376
 1377 Though it is possible to intentionally create an Assertion designed to be presented to multiple
 1378 RPs, this method can lead to lax audience restriction of the Assertion itself, which in turn could
 1379 lead to privacy and security breaches for the Subscriber across these RPs. Such multi-RP use is
 1380 not recommended. Instead, RPs are encouraged to fetch their own individual Assertions.

1381
 1382 The RP must protect itself against injection of manufactured or captured Assertions by use of
 1383 cross-site scripting protection or other accepted techniques. Claims within the Assertion must
 1384 be validated including issuer verification, signature validation, and audience restriction.
 1385 Conveyance of the Assertion from the IdP to the Subscriber as well as from the Subscriber to
 1386 the RP must be made over an authenticated protected channel.

1387 Assertion Proxying

1388 In some implementations, a proxy accepts an Assertion from the IdP and creates a derived
 1389 Assertion when interacting directly with the RP, acting as an intermediary between the
 1390 Subscriber, the IdP, and the RP. From the perspective of the true IdP, the proxy is a single RP.
 1391 From the perspective of the true RPs, the proxy is a single IdP.

1392 There are several common reasons for such proxies:

- 1393 • Portals that provide users access to multiple RPs that require user authentication
- 1394 • Web caching mechanisms that are required to satisfy the RP's access control policies,
 1395 especially when mutually-authenticated TLS with the Subscriber is used
- 1396 • Network monitoring and/or filtering mechanisms that terminate TLS in order to inspect
 1397 and manipulate the traffic

1398
 1399 Conveyance of all information must be made over authenticated protected channels.

1400 Assertion Security

1401 IdPs, RPs, Subscribers, and parties outside of a typical Assertions transaction may be malicious
 1402 or become compromised. An attacker might have an interest in modifying or replacing an
 1403 Assertion to obtain a greater level of access to a resource or service provided by an RP. They
 1404 might be interested in obtaining or modifying Assertions and Assertion references to
 1405 impersonate a Subscriber or access unauthorized data or services.

1406 Furthermore, it is possible that two or more entities may be colluding to attack another party.
 1407 An attacker may attempt to subvert Assertion protocols by directly compromising the integrity
 1408 or confidentiality of the Assertion data. For the purpose of these types of threats, authorized
 1409 parties who attempt to exceed their privileges may be considered attackers.

1410 Common attacks against Assertion transmission transactions include the following:

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

Formatted: Font: 13 pt

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

- 1417
- 1418
- 1419
- 1420
- 1421
- 1422
- 1423
- 1424
- 1425
- 1426
- 1427
- 1428
- 1429
- 1430
- 1431
- 1432
- 1433
- 1434
- 1435
- 1436
- Assertion Manufacture/Modification: An attacker generates a forged Assertion or modifies the content of an existing Assertion (such as the authentication or attribute statements), causing the RP to grant inappropriate access to the Subscriber. For example, an attacker may modify the Assertion to extend the validity period and keep using an Assertion; or a Subscriber may modify the Assertion to have access to information that they should not be able to view.
 - Assertion Disclosure: Assertions may contain authentication and attribute statements that include sensitive Subscriber information. Disclosure of the Assertion contents can make the Subscriber vulnerable to other types of attacks.
 - Assertion Repudiation by the IdP: An Assertion may be repudiated by an IdP if the proper mechanisms are not in place. For example, if an IdP does not digitally sign an Assertion, the IdP can claim that it was not generated through the services of the IdP.
 - Assertion Repudiation by the Subscriber: Since it is possible for a compromised or malicious IdP to issue Assertions to the wrong party, a Subscriber can repudiate any transaction with the RP that was authenticated using only a bearer Assertion.
 - Assertion Redirect: An attacker uses the Assertion generated for one RP to obtain access to a second RP.
 - Assertion Reuse: An attacker attempts to use an Assertion that has already been used once with the intended RP.

1437 In some cases, the Subscriber is issued some secret information so that they can be recognized by the RP. The knowledge of this information distinguishes the Subscriber from attackers who wish to impersonate the them. In the case of Holder-of-Key Assertions, this secret could already have been established with the IdP prior to the initiation of the Assertion protocol.

1442 In other cases, the IdP will generate a temporary secret and transmit it to the authenticated Subscriber for this purpose. When this secret is used to authenticate to the RP, this temporary secret will be referred to as a secondary authenticator. Secondary authenticators include Assertions in the direct model, session keys in Kerberos, Assertion references in the indirect model, and cookies used for authentication.

1448 Threats to the secondary authenticator include the following:

- 1449
- 1450
- 1451
- 1452
- 1453
- 1454
- 1455
- 1456
- 1457
- 1458
- 1459
- Secondary Authenticator Manufacture: An attacker may attempt to generate a valid secondary authenticator and use it to impersonate a Subscriber.
 - Secondary Authenticator Capture: An attacker may use a session hijacking attack to capture the secondary authenticator when the IdP transmits it to the Subscriber after the primary authentication step, or the attacker may use a man-in-the-middle attack to obtain the secondary authenticator as it is being used by the Subscriber to authenticate to the RP. If, as in the indirect model, the RP needs to send the secondary authenticator back to the IdP in order to check its validity or obtain the corresponding Assertion data, an attacker may similarly subvert the communication protocol between the IdP and the RP to capture a secondary authenticator. In any of the above scenarios, the secondary authenticator can be used to impersonate the Subscriber.

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"

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

1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500

Finally, in order for the Subscriber’s authentication to the RP to be useful, the binding between the secret used to authenticate to the RP and the Assertion data referring to the Subscriber needs to be strong. In Assertion substitution, a Subscriber may attempt to impersonate a more privileged Subscriber by subverting the communication channel between the IdP and RP, for example by reordering the messages, to convince the RP that their secondary authenticator corresponds to Assertion data sent on behalf of the more privileged Subscriber.

Threat Mitigation Strategies

Mitigation techniques are described below for each of the threats described in the last subsection:

- Assertion Manufacture/Modification: To mitigate this threat, the following mechanisms are used:
 - The Assertion is digitally signed by the IdP. The RP checks the digital signature to verify that it was issued by a legitimate IdP.
 - The Assertion is sent over a protected session such as TLS. In order to protect the integrity of Assertions from malicious attack, the IdP is authenticated.
 - The Assertion contains a non-guessable random identifier.
- Assertion Disclosure: To mitigate this threat, one of the following mechanisms are used:
 - The Assertion is sent over a protected session to an authenticated RP. Note that, in order to protect Assertions against both disclosure and manufacture/modification using a protected session, both the RP and the IdP need to be validated.
 - Assertions are signed by the IdP and encrypted for a specific RP. It should be noted that this provides all the same guarantees as a mutually authenticated protected session, and may therefore be considered equivalent. The general requirement for protecting against both Assertion disclosure and Assertion manufacture/modification may therefore be described as a mutually authenticated protected session or equivalent between the IdP and the RP.
- Assertion Repudiation by the IdP: To mitigate this threat, the Assertion is digitally signed by the IdP using a key that supports non-repudiation. The RP checks the digital signature to verify that it was issued by a legitimate IdP.
- Assertion Repudiation by the Subscriber: To mitigate this threat, the IdP issues holder-of-key Assertions, rather than bearer Assertions. The Subscriber can then prove possession of the asserted key to the RP. If the asserted key matches the Subscriber’s presented key, it will be proof to all parties involved that it was the Subscriber who authenticated to the RP rather than a compromised IdP impersonating the Subscriber.
- Assertion Redirect: To mitigate this threat, the Assertion includes the identity of the RP for which it was generated. The RP verifies that incoming Assertions include its identity as the recipient of the Assertion.

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

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

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

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

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

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

- 1501 • Assertion Reuse: To mitigate this threat, the following mechanisms are used:
 - 1502 ○ The Assertion includes a timestamp and has a short lifetime of validity. The RP
 - 1503 checks the timestamp and lifetime values to ensure the Assertion is currently valid.
 - 1504 ○ The RP keeps track of Assertions that were consumed within a (configurable) time
 - 1505 window to ensure that an Assertion is not used more than once within that time
 - 1506 window.
 - 1507 • Secondary Authenticator Manufacture: To mitigate this threat, one of the following
 - 1508 mechanisms is used:
 - 1509 ○ The secondary authenticator may contain sufficient entropy that an attacker without
 - 1510 direct access to the IdP’s random number generator cannot guess the value of a
 - 1511 valid secondary authenticator.
 - 1512 ○ The secondary authenticator may contain timely Assertion data that is signed by the
 - 1513 IdP or integrity protected using a key shared between the IdP and the RP.
 - 1514 • Secondary Authenticator Capture: To mitigate this threat, adequate protections are in
 - 1515 place throughout the lifetime of any secondary authenticators used in the Assertion
 - 1516 protocol:
 - 1517 ○ In order to protect the secondary authenticator while it is in transit between the IdP
 - 1518 and the Subscriber, the secondary authenticator is sent via a protected session
 - 1519 established during the primary authentication of the Subscriber.
 - 1520 ○ In order to protect the secondary authenticator from capture as it is submitted to
 - 1521 the RP, the secondary authenticator is used in an authentication protocol which
 - 1522 protects against eavesdropping and man-in-the-middle attacks.
 - 1523 ○ In order to protect the secondary authenticator after it has been used, it is never
 - 1524 transmitted over an unprotected session or to an unauthenticated party while it is
 - 1525 still valid.
 - 1526 • Assertion Substitution: To mitigate this threat, one of the following mechanisms is used:
 - 1527 ○ Responses to Assertion requests contain the value of the Assertion reference used in
 - 1528 the request or some other nonce that was cryptographically bound to the request by
 - 1529 the RP.
 - 1530 ○ Responses to Assertion requests are bound to the corresponding requests by
 - 1531 message order, as in HTTP, provided that Assertions and requests are protected by a
 - 1532 protocol such as TLS that can detect and disallow malicious reordering of packets.

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

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

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

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

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

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

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

Formatted: List Paragraph, Indent: Left: 0.5", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1"

Formatted: Font: 13 pt

Assertion Examples

The following represent three (3) types of Assertion technologies: Security Assertion Markup Language (SAML) Assertions, Kerberos tickets, and OpenID Connect tokens.

Security Assertion Markup Language (SAML)

SAML is an XML-based framework for creating and exchanging authentication and Attribute information between trusted entities over the internet. As of this writing, the latest specification for [SAML] is SAML v2.0, issued 15 March 2005.

The building blocks of SAML include:

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

1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585

- [Assertion XML schema which defines the structure of the Assertion](#)
- [SAML Protocols which are used to request Assertions and artifacts](#)
- [Bindings that define the underlying communication protocols \(such as HTTP or SOAP\) and can be used to transport the SAML Assertions.](#)

[The three components above define a SAML profile that corresponds to a particular use case such as “Web Browser SSO.” SAML Assertions are encoded in an XML schema and can carry up to three types of statements:](#)

- [Authentication statements include information about the Assertion issuer, the authenticated Subscriber, validity period, and other authentication information. For example, an Authentication Assertion would state the Subscriber “John” was authenticated using a password at 10:32 p.m. on 06-06-2004.](#)
- [Attribute statements contain specific additional characteristics related to the Subscriber. For example, subject “John” is associated with attribute “Role” with value “Manager.”](#)
- [Authorization statements identify the resources the Subscriber has permission to access. These resources may include specific devices, files, and information on specific web servers. For example, subject “John” for action “Read” on “Webserver1002” given evidence “Role.”](#)

[Kerberos Tickets](#)

[The Kerberos Network Authentication Service \[RFC 4120\] was designed to provide strong authentication for client/server applications using symmetric-key cryptography on a local, shared network. Extensions to Kerberos can support the use of public key cryptography for selected steps of the protocol. Kerberos also supports confidentiality and integrity protection of session data between the Subscriber and the RP. Even though Kerberos uses Assertions, since it is designed for use on shared networks it is not truly a federation protocol.](#)

[Kerberos supports authentication of a Subscriber over an untrusted, shared local network using one or more IdPs. The Subscriber implicitly authenticates to the IdP by demonstrating the ability to decrypt a random session key encrypted for the Subscriber by the IdP. \(Some Kerberos variants also require the Subscriber to explicitly authenticate to the IdP, but this is not universal.\)](#)

[In addition to the encrypted session key, the IdP also generates another encrypted object called a Kerberos ticket. The ticket contains the same session key, the identity of the Subscriber to whom the session key was issued, and an expiration time after which the session key is no longer valid. The ticket is confidentiality and integrity protected by a pre-established that is key shared between the IdP and the RP during an explicit setup phase.](#)

[To authenticate using the session key, the Subscriber sends the ticket to the RP along with encrypted data that proves that the Subscriber possesses the session key embedded within the](#)

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"

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

1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628

Kerberos ticket. Session keys are either used to generate new tickets, or to encrypt and authenticate communications between the Subscriber and the RP.

To begin the process, the Subscriber sends an authentication request to the Authentication Server (AS). The AS encrypts a session key for the Subscriber using the Subscriber’s long term Credential. The long term Credential may either be a secret key shared between the AS and the Subscriber, or in the PKINIT variant of Kerberos, a Public Key Certificate. It should be noted that most variants of Kerberos based on a Shared Secret key between the Subscriber and IdP derive this key from a user generated password. As such, they are vulnerable to offline dictionary attack by a passive eavesdropper.

In addition to delivering the session key to the Subscriber, the AS also issues a ticket using a key it shares with the Ticket Granting Server (TGS). This ticket is referred to as a Ticket Granting Ticket (TGT), since the verifier uses the session key in the TGT to issue tickets rather than to explicitly authenticate the verifier. The TGS uses the session key in the TGT to encrypt a new session key for the Subscriber and uses a key it shares with the RP to generate a ticket corresponding to the new session key. The Subscriber decrypts the session key and uses the ticket and the new session key together to authenticate to the RP.

OpenID Connect

OpenID Connect is an internet-scale federated identity and authentication protocol built on top of the OAuth 2.0 authorization framework and the JSON Object Signing and Encryption (JOSE) cryptographic system. As of this writing, the latest specification is version 1.0 with errata, dated November 8, 2014.

OpenID Connect builds on top of the OAuth 2.0 authorization protocol to enable the Subscriber to authorize the RP to access the Subscriber’s identity and authentication information. The RP in both OpenID Connect and OAuth 2.0 is known as the client.

In a successful OpenID Connect transaction, the IdP issues an ID Token, which is a signed Assertion in JSON Web Token (JWT) format. The client parses the ID Token to learn about the Subscriber and primary authentication event at the IdP. This token contains at minimum the following claims about the Subscriber and authentication event:

- iss : HTTPS URL identifying the IdP that issued the Assertion
- sub : IdP-specific subject identifier representing the Subscriber
- aud : IdP-specific audience identifier, equal to the OAuth 2.0 client identifier of the client at the IdP
- exp : Timestamp at which the Identity token expires and after which must not be accepted the client
- iat : Timestamp at which the Identity token was issued and before which must not be accepted by the client

Formatted: Font: Courier, 10 pt, Font color: Red, Highlight

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

Formatted: Font: (Default) Courier, 10 pt, Font color: Red, Highlight

Formatted: Font: Courier, 10 pt, Font color: Red, Highlight

Formatted: Font: Courier, 10 pt, Font color: Red, Highlight

Formatted: Font: Courier, 10 pt, Font color: Red, Highlight

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

1629 In addition to the Identity token, the IdP also issues the client an OAuth 2.0 access token which
1630 can be used to access the UserInfo Endpoint at the IdP. This endpoint returns a JSON object
1631 representing a set of claims about the Subscriber, including but not limited to their name, email
1632 address, physical address, phone number, and other profile information.

1633
1634 While the information inside the ID Token is reflective of the authentication event, the
1635 information in the UserInfo Endpoint is generally more stable and could be more general
1636 purpose. Access to different claims from the UserInfo Endpoint is governed by the use of a
1637 specially defined set of OAuth scopes, openid, profile, email, phone, and address. An
1638 additional scope, offline_access, is used to govern the issuance of refresh tokens, which
1639 allow the RP to access the UserInfo Endpoint when the Subscriber is not present.

DRAFT

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

1640 In addition, certain registration, identity proofing, and issuance processes performed by the
1641 credential service provider (CSP) may be delegated to an entity known as the registration
1642 authority (RA) or identity manager (IM). A close relationship between the RA/IM and CSP is
1643 typical, and the nature of this relationship may differ among RAs, IMs, and CSPs. The minimum
1644 specifications defined in this document assume that relationships between participants and
1645 their requirements are established in the trust framework for the identity management system.

1646
1647 Electronic authentication begins with registration (also referred to as enrollment). The usual
1648 sequence for registration proceeds as follows. An applicant applies to a CSP. If approved, the
1649 CSP creates a credential and binds it to one or more authenticators. The credential includes an
1650 identifier, which can be pseudonymous, and one or more attributes that the CSP has verified.
1651 The authenticators may be issued by the CSP, generated/provided directly by the subscriber, or
1652 provided by a third party. The authenticator and credential may be used in subsequent
1653 authentication events.

1654
1655 The process used to verify an applicant's association with their real world identity is called
1656 identity proofing. The strength of identity proofing is described by a categorization called the
1657 identity assurance level (IAL, see subsection on Assurance Level Model below in this document).
1658 Minimum specifications for identity proofing and verification during the registration process
1659 have been established in *ITRM Guidance Document: Identity Proofing and Verification*.

1660
1661 At IAL 1, identity proofing is not required, therefore any attribute information provided by the
1662 subscriber is self-asserted and not verified. At IAL 2 and 3, identity proofing is required, but the
1663 CSP may assert verified attribute values, verified attribute claims, pseudonymous identifiers, or
1664 nothing. This information assists Relying Parties (RPs) in making access control or authorization
1665 decisions. RPs may decide that their required IAL is 2 or 3, but may only need specific
1666 attributes, and perhaps attributes that retain an individual's pseudonymity. A relying party may
1667 also employ a federated identity approach where the RP outsources all identity proofing,
1668 attribute collection, and attribute storage to a CSP.

1669
1670 In these minimum specifications, the party to be authenticated is called a claimant and the
1671 party verifying that identity is called a verifier. When a claimant successfully demonstrates
1672 possession and control of one or more authenticators to a verifier through an authentication
1673 protocol, the verifier can verify that the claimant is a valid subscriber. The verifier passes on an
1674 assertion about the subscriber, who may be either pseudonymous or non-pseudonymous, to
1675 the RP. That assertion includes an identifier, and may include identity information about the
1676 subscriber, such as the name, or other attributes that were verified in the enrollment process
1677 (subject to the policies of the CSP and the trust framework for the system). When the verifier is
1678 also the RP, the assertion may be implicit. The RP can use the authenticated information
1679 provided by the verifier to make access control or authorization decisions.

1680
1681 Authentication establishes confidence in the claimant's identity, and in some cases in the
1682 claimant's attributes. Authentication does not determine the claimant's authorizations or
1683 access privileges; this is a separate decision. RPs will use a subscriber's authenticated identity

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

1684 and attributes with other factors to make access control or authorization decisions. Nothing in
1685 this document precludes RPs from requesting additional information from a subscriber that has
1686 successfully authenticated.

1687
1688 The strength of the authentication process is described by a categorization called the
1689 authenticator assurance level (AAL). AAL 1 requires single-factor authentication and is
1690 permitted with a variety of different authenticator types. At AAL 2, authentication requires two
1691 authentication factors for additional security. Authentication at the highest level, AAL 3,
1692 requires the use of a hardware-based authenticator and one other factor.

1693
1694 As part of authentication, mechanisms such as device identity or geo-location may be used to
1695 identify or prevent possible authentication false positives. While these mechanisms do not
1696 directly increase the authenticator assurance level, they can enforce security policies and
1697 mitigate risks. In many cases, the authentication process and services will be shared by many
1698 applications and agencies. However, it is the individual agency or application acting as the RP
1699 that shall make the decision to grant access or process a transaction based on the specific
1700 application requirements.

1701 1702 Authentication Components and Process Flows

1703
1704 The various entities and interactions that comprise the electronic authentication model defined
1705 in these minimum specifications have been illustrated below in **Figure 1**. The left shows the
1706 enrollment, credential issuance, lifecycle management activities, and the stages an individual
1707 transitions, based on the specific phase of the identity proofing and authentication process.

1708
1709 The authentication process begins with the claimant demonstrating to the verifier possession
1710 and control of an authenticator that is bound to the asserted identity through an authentication
1711 protocol. Once possession and control have been demonstrated, the verifier confirms that the
1712 credential remains valid, usually by interacting with the CSP.

1713
1714 The exact nature of the interaction between the verifier and the claimant during the
1715 authentication protocol contributes to the overall security of the system. Well-designed
1716 protocols can protect the integrity and confidentiality of traffic between the claimant and the
1717 verifier both during and after the authentication exchange, and it can help limit the damage
1718 that can be done by an attacker masquerading as a legitimate verifier.

1719
1720 Additionally, mechanisms located at the verifier can mitigate online guessing attacks against
1721 lower entropy secrets like passwords and PINs by limiting the rate at which an attacker can
1722 make authentication attempts or otherwise delaying incorrect attempts. Generally, this is done
1723 by keeping track of and limiting the number of unsuccessful attempts, since the premise of an
1724 online guessing attack is that most attempts will fail.

1725
1726 The verifier is a functional role, but is frequently implemented in combination with the CSP
1727 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

1728 that the verifier does not learn the subscriber's authenticator secret in the process of
1729 authentication, or at least to ensure that the verifier does not have unrestricted access to
1730 secrets stored by the CSP.

1731
1732 The usual sequence of interactions in the authentication process is as follows:

- 1733 1. An applicant applies to a CSP through a registration process.
- 1734 2. The CSP identity proofs that applicant. Upon successful proofing, the applicant becomes
1735 a subscriber.
- 1736 3. An authenticator and a corresponding credential are established between the CSP and
1737 the new subscriber.
- 1738 4. The CSP maintains the credential, its status, and the enrollment data collected for the
1739 lifetime of the credential. The subscriber maintains his or her authenticator.

1740
1741 Other sequences are less common, but could also achieve the same functional requirements.
1742 The right side of Figure 1 shows the entities and the interactions related to using an
1743 authenticator to perform electronic authentication. When the subscriber needs to authenticate
1744 to perform a transaction, he or she becomes a claimant to a verifier. The interactions are as
1745 follows:

- 1746 1. The claimant proves to the verifier that he or she possesses and controls the
1747 authenticator through an authentication protocol.
- 1748 2. The verifier interacts with the CSP to validate the credential that binds the subscriber's
1749 identity to his or her authenticator and to optionally obtain claimant attributes.
- 1750 3. If the verifier is separate from the RP (application), the verifier provides an assertion
1751 about the subscriber to the RP, which may use the information in the assertion to make
1752 an access control or authorization decision.
- 1753 4. An authenticated session is established between the subscriber and the RP.

1754
1755 In all cases, the RP should request the attributes it requires from a CSP prior to authentication
1756 of the claimant. In addition, the claimant should be requested to consent to the release of
1757 those attributes prior to generation and release of an assertion.

1758
1759 In some cases, the verifier does not need to communicate in real time with the CSP to complete
1760 the authentication activity (e.g., some uses of digital certificates). Therefore, the dashed line
1761 between the verifier and the CSP represents a logical link between the two entities rather than
1762 a physical link. In some implementations, the verifier, RP and the CSP functions may be
1763 distributed and separated as shown in Figure 1; however, if these functions reside on the same
1764 platform, the interactions between the components are local messages between applications
1765 running on the same system rather than protocols over shared untrusted networks.

1766
1767 As noted above, CSPs maintain status information about issued credentials. CSPs may assign a
1768 finite lifetime to a credential in order to limit the maintenance period. When the status
1769 changes, or when the credentials near expiration, credentials may be renewed or re-issued; or,
1770 the credential may be revoked or destroyed. Typically, the subscriber authenticates to the CSP
1771 using his or her existing, unexpired authenticator and credential in order to request issuance of

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

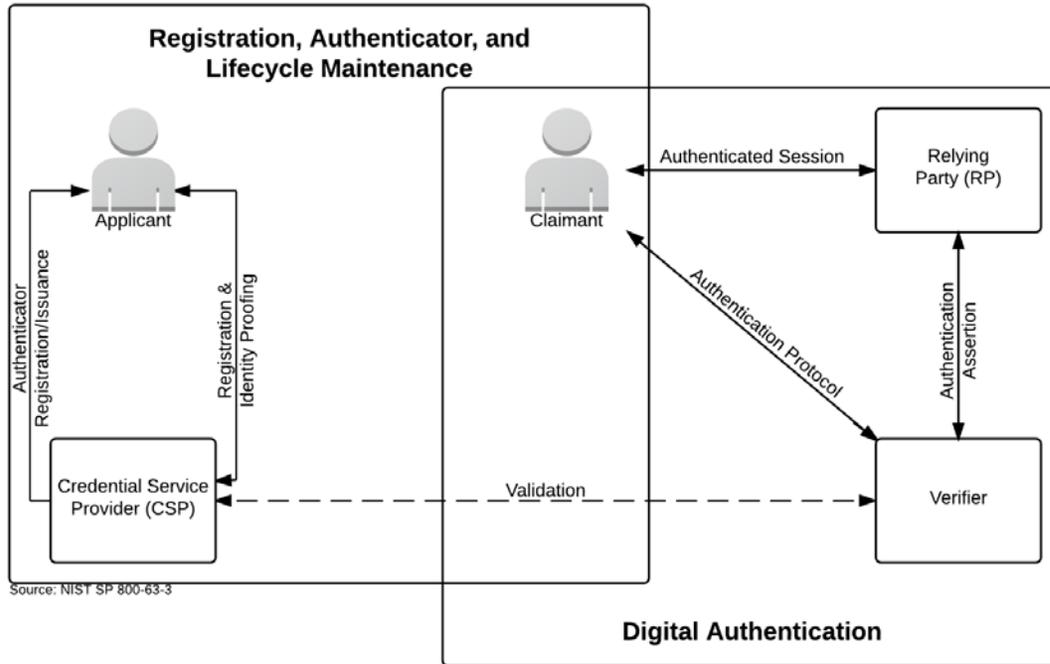
1772 a new authenticator and credential. If the subscriber fails to request authenticator and
1773 credential re-issuance prior to their expiration or revocation, he or she may be required to
1774 repeat the enrollment process to obtain a new authenticator and credential. Alternatively, the
1775 CSP may choose to accept a request during a grace period after expiration.

DRAFT

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

1776

Figure 1. Electronic Authentication Model



1777
1778
1779
1780
1781
1782
1783
1784

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.

1785 Authentication Protocols and Lifecycle Management

1786

1787 Authenticators

1788 The established paradigm for electronic authentication identifies three factors as the
1789 cornerstone of authentication:

- 1790 • ~~Something you know (for example, a password)~~
- 1791 • ~~Something you have (for example, an ID badge or a cryptographic key)~~
- 1792 • ~~Something you are (for example, a fingerprint or other biometric data)~~

1793

1794 Multi-factor authentication refers to the use of more than one of the factors listed
1795 above. The strength of authentication systems is largely determined by the number of
1796 factors incorporated by the system. Implementations that use two different factors are
1797 considered to be stronger than those that use only one factor; systems that incorporate
1798 all three factors are stronger than systems that only incorporate two of the factors.
1799 Other types of information, such as location data or device identity, may be used by an
1800 RP or verifier to evaluate the risk in a claimed identity, but they are not considered
1801 authentication factors.

1802

1803 In electronic authentication the claimant possesses and controls one or more
1804 authenticators that have been registered with the CSP and are used to prove the
1805 claimant's identity. The authenticator(s) contains secrets the claimant can use to prove
1806 that he or she is a valid subscriber, the claimant authenticates to a system or application
1807 over a network by proving that he or she has possession and control of an
1808 authenticator.

1809

1810 The secrets contained in authenticators are based on either public key pairs
1811 (asymmetric keys) or shared secrets (symmetric keys). A public key and a related private
1812 key comprise a public key pair. The private key is stored on the authenticator and is
1813 used by the claimant to prove possession and control of the authenticator. A verifier,
1814 knowing the claimant's public key through some credential (typically a public key
1815 certificate), can use an authentication protocol to verify the claimant's identity, by
1816 proving that the claimant has possession and control of the associated private key
1817 authenticator.

1818

1819 Shared secrets stored on authenticators may be either symmetric keys or passwords.
1820 While they can be used in similar protocols, one important difference between the two
1821 is how they relate to the subscriber. While symmetric keys are generally stored in
1822 hardware or software that the subscriber controls, passwords are intended to be
1823 memorized by the subscriber. As such, keys are something the subscriber has, while
1824 passwords are something he or she knows. Since passwords are committed to memory,

Formatted: Font: 13 pt

1825 they usually do not have as many possible values as cryptographic keys, and, in many
1826 protocols, are severely vulnerable to network attacks that are more restricted for keys.

1827
1828 Moreover, the entry of passwords into systems (usually through a keyboard) presents
1829 the opportunity for very simple keyboard logging attacks, and may also allow those
1830 nearby to learn the password by watching it being entered. Therefore, keys and
1831 passwords demonstrate somewhat separate authentication properties (something you
1832 have rather than something you know). When using either public key pairs or shared
1833 secrets, the subscriber has a duty to maintain exclusive control of his or her
1834 authenticator, since possession and control of the authenticator is used to authenticate
1835 the claimant's identity.

1836
1837 The minimum specifications defined in this document assume that authenticators
1838 always contain a secret. Authentication factors classified as something you know are not
1839 necessarily secrets. Knowledge based authentication, where the claimant is prompted
1840 to answer questions that can be confirmed from public databases, also does not
1841 constitute an acceptable secret for electronic authentication. More generally,
1842 something you are does not generally constitute a secret. However, the requirements
1843 for some identity management systems may allow the use of biometrics as an
1844 authenticator.

1845
1846 Biometric characteristics are unique personal attributes that can be used to verify the
1847 identity of a person who is physically present at the point of verification. They include
1848 facial features, fingerprints, iris patterns, voiceprints, and many other characteristics.
1849 NIST recommends that biometrics be used in the enrollment process for higher levels of
1850 assurance to later help prevent a subscriber who is registered from repudiating the
1851 enrollment, to help identify those who commit enrollment fraud, and to unlock
1852 authenticators. The specific requirements for the use of biometrics must be defined in
1853 the trust framework for the system.

1854
1855 The minimum specifications in this document encourage identity management systems
1856 to use authentication processes and protocols that incorporate all three factors, as a
1857 means of enhancing system security. An electronic authentication system may
1858 incorporate multiple factors in either of two ways. The system may be implemented so
1859 that multiple factors are presented to the verifier, or some factors may be used to
1860 protect a secret presented to the verifier. If multiple factors are presented to the
1861 verifier, each will need to be an authenticator (and therefore contain a secret). If a
1862 single factor is presented to the verifier, the additional factors are used to protect the
1863 authenticator and need not themselves be authenticators.

1864

1865 **Credentials**

1866 As described in the preceding sections, credentials bind an authenticator to the
1867 subscriber as part of the issuance process. Credentials are stored and maintained by the
1868 CSP. The claimant possesses an authenticator, but is not necessarily in possession of the
1869 electronic credentials. For example, database entries containing the user attributes are
1870 considered to be credentials for the purpose of this document but are possessed by the
1871 verifier.

1872
1873 **Assertions**

1874 Upon completion of the electronic authentication process, the verifier generates an
1875 assertion containing the result of the authentication and provides it to the RP. If the
1876 verifier is implemented in combination with the RP, the assertion is implicit. If the
1877 verifier is a separate entity from the RP, as in typical federated identity models, the
1878 assertion is used to communicate the result of the authentication process, and
1879 optionally information about the subscriber, from the verifier to the RP.
1880 Assertions may be communicated directly to the RP, or can be forwarded through the
1881 subscriber, which has further implications for system design. An RP trusts an assertion
1882 based on the source, the time of creation, and the corresponding trust framework that
1883 governs the policies and process of CSPs and RPs. The verifier is responsible for
1884 providing a mechanism by which the integrity of the assertion can be confirmed.

1885
1886 The RP is responsible for authenticating the source (e.g., the verifier) and for confirming
1887 the integrity of the assertion. When the verifier passes the assertion through the
1888 subscriber, the verifier must protect the integrity of the assertion in such a way that it
1889 cannot be modified by the subscriber. However, if the verifier and the RP communicate
1890 directly, a protected session may be used to provide the integrity protection. When
1891 sending assertions across a network, the verifier is responsible for ensuring that any
1892 sensitive subscriber information contained in the assertion can only be extracted by an
1893 RP that it trusts to maintain the information's confidentiality.

1894
1895 **Examples of assertions include:**

- 1896 • ~~SAML Assertions~~—SAML assertions are specified using a mark-up language
1897 intended for describing security assertions. They can be used by a verifier to
1898 make a statement to an RP about the identity of a claimant. SAML assertions may
1899 be digitally signed.
- 1900 • ~~OpenID Connect Claims~~—OpenID Connect are specified using JavaScript Object
1901 Notation (JSON) for describing security, and optionally, user claims. JSON user
1902 info claims may be digitally signed.

1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918

~~• Kerberos Tickets — Kerberos Tickets allow a ticket granting authority to issue session keys to two authenticated parties using symmetric key based encapsulation schemes.~~

~~Relying Parties~~

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

- Formatted: Font: Not Bold
- Formatted: Font: 13 pt, Not Bold
- Formatted: Font: Not Bold

DRAFT

1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956

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.¹⁴ 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.¹⁵

¹⁴ 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.

¹⁵ Approved cryptographic techniques shall must be FIPS approved, NIST recommended, or otherwise compliant with Commonwealth IT Information Security Standard (SEC501):

Formatted: Font: 13 pt, Not Bold

Formatted: Normal

Formatted: Font: Not Bold

1957 Authenticator Assurance Level 3 – AAL 3 is intended to provide the highest practical electronic
 1958 authentication assurance. Authentication at AAL 3 is based on proof of possession of a key
 1959 through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only “hard”
 1960 cryptographic authenticators are allowed. The authenticator is required to be a hardware
 1961 cryptographic module validated at Federal Information Processing Standard (FIPS) 140 Level 2
 1962 or higher overall with at least FIPS 140 Level 3 physical security. AAL 3 authenticator
 1963 requirements can be met by using the PIV authentication key of a FIPS 201 compliant Personal
 1964 Identity Verification (PIV) Card.

1965 **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

1968

1969 Privacy and Security

1970

1971 The minimum specifications established in this document for privacy and security in the use of
 1972 person information for ~~electronic authentication~~Electronic Authentication apply the Fair
 1973 Information Practice Principles (FIPPs).¹⁶ The FIPPs have been endorsed by the National
 1974 Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.¹⁷

1975

1976 The minimum specifications also adhere to the Identity Ecosystem Framework (IDEF) Baseline
 1977 Functional Requirements (v.1.0) for privacy and security, adopted by the Identity Ecosystem
 1978 Steering Group (IDESG) in October 2015 (**Appendix 2**).

1979

1980 The minimum specifications for ~~identity proofing~~Assertions and verification apply the following
 1981 FIPPs:

- 1982 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants
 1983 regarding collection, use, dissemination, and maintenance of person information required
 1984 during the ~~registration~~Registration, ~~identity proofing~~Identity Proofing and verification
 1985 processes.
- 1986 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using
 1987 person information and, to the extent practicable, seek consent for the collection, use,
 1988 dissemination, and maintenance of that information. RAs and CSPs also should provide
 1989 mechanisms for appropriate access, correction, and redress of person information.
- 1990 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits
 1991 the collection of person information and specifically articulate the purpose or purposes for
 1992 which the information is intended to be used.
- 1993 • Data Minimization: RAs and CSPs should collect only the person information directly
 1994 relevant and necessary to accomplish the ~~registration~~Registration and related processes,
 1995 and only retain that information for as long as necessary to fulfill the specified purpose.
- 1996 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for
 1997 the purpose specified in the notice. Disclosure or sharing that information should be limited
 1998 to the specific purpose for which the information was collected.
- 1999 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that
 2000 person information is accurate, relevant, timely, and complete.
- 2001 • Security: RAs and CSPs should protect personal information through appropriate security
 2002 safeguards against risks such as loss, unauthorized access or use, destruction, modification,
 2003 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>.

2004 | ●—Accountability and Auditing: RAs and CSPs should be accountable for complying with these
 2005 | principles, providing training to all employees and contractors who use person information,
 2006 | and auditing the actual use of person information to demonstrate compliance with these
 2007 | principles and all applicable privacy protection requirements.

2008 | **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.~~

~~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.~~

~~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.~~

~~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~~

2047
2048
2049
2050

~~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

2051 Appendix 1. IMSAC Charter

2052

2053

**COMMONWEALTH OF VIRGINIA
IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL
CHARTER**

2054

2055

2056

2057

Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)

2058

2059

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.

2060

2061

2062

2063

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 parties on identity credentials, as defined in § 59.1-550.

2064

2065

2066

2067

2068

2069

2070

2071

Membership and Governance Structure (§ 2.2-437.B)

2072

2073

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

2074

2075

2076

2077

2078

2079

2080

2081

1. The Advisory Council consists of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology. Members include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.

2082

2083

2084

2085

2086

2. The Advisory Council designates one of its members as chairman.

3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.

2087

2088

2089

4. Members serve without compensation but may be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

2090

2091

2092

5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

2093 The formation, membership and governance structure for the Advisory Council has been
2094 codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

2095
2096 The statutory authority and requirements for public notice and comment periods for guidance
2097 documents have been established pursuant to § 2.2-437.C, as follows:

2098
2099 C. Proposed guidance documents and general opportunity for oral or written submittals as to
2100 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published
2101 in the Virginia Register of Regulations as a general notice following the processes and
2102 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§
2103 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written
2104 comments following the posting and publication and shall hold at least one meeting dedicated
2105 to the receipt of oral comment no less than 15 days after the posting and publication. The
2106 Advisory Council shall also develop methods for the identification and notification of interested
2107 parties and specific means of seeking input from interested persons and groups. The Advisory
2108 Council shall send a copy of such notices, comments, and other background material relative to
2109 the development of the recommended guidance documents to the Joint Commission on
2110 Administrative Rules.

2111
2112
2113 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the
2114 minutes of the meeting and related IMSAC documents, visit:
2115 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

2116 Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline
2117 Functional Requirements (v.1.0) for Privacy and Security

2118

2119 PRIVACY-1. DATA MINIMIZATION

2120 Entities MUST limit the collection, use, transmission and storage of personal information to the
2121 minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities
2122 providing claims or attributes MUST NOT provide any more personal information than what is
2123 requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to
2124 accommodate information requests of variable granularity, to support data minimization.

2125

2126 PRIVACY-2. PURPOSE LIMITATION

2127 Entities MUST limit the use of personal information that is collected, used, transmitted, or
2128 stored to the specified purposes of that transaction. Persistent records of contracts, assurances,
2129 consent, or legal authority MUST be established by entities collecting, generating, using,
2130 transmitting, or storing personal information, so that the information, consistently is used in
2131 the same manner originally specified and permitted.

2132

2133 PRIVACY-3. ATTRIBUTE MINIMIZATION

2134 Entities requesting attributes MUST evaluate the need to collect specific attributes in a
2135 transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST
2136 collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever
2137 feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities
2138 MUST be bound to claims instead of actual attribute values.

2139

2140 PRIVACY-4. CREDENTIAL LIMITATION

2141 Entities MUST NOT request USERS' credentials unless necessary for the transaction and then
2142 only as appropriate to the risk associated with the transaction or to the risks to the parties
2143 associated with the transaction.

2144

2145 PRIVACY-5. DATA AGGREGATION RISK

2146 Entities MUST assess the privacy risk of aggregating personal information, in systems and
2147 processes where it is collected, generated, used, transmitted, or stored, and wherever feasible,
2148 MUST design and operate their systems and processes to minimize that risk. Entities MUST
2149 assess and limit linkages of personal information across multiple transactions without the
2150 USER's explicit consent.

2151

2152 PRIVACY-6. USAGE NOTICE

2153 Entities MUST provide concise, meaningful, and timely communication to USERS describing how
2154 they collect, generate, use, transmit, and store personal information.

2155

2156 PRIVACY-7. USER DATA CONTROL

2157 Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete
2158 personal information.

2159 PRIVACY-8. THIRD-PARTY LIMITATIONS

2160 Wherever USERS make choices regarding the treatment of their personal information, those
2161 choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it
2162 transmits the personal information.

2163

2164 PRIVACY-9. USER NOTICE OF CHANGES

2165 Entities MUST, upon any material changes to a service or process that affects the prior or
2166 ongoing collection, generation, use, transmission, or storage of USERS' personal information,
2167 notify those USERS, and provide them with compensating controls designed to mitigate privacy
2168 risks that may arise from those changes, which may include seeking express affirmative consent
2169 of USERS in accordance with relevant law or regulation.

2170

2171 PRIVACY-10. USER OPTION TO DECLINE

2172 USERS MUST have the opportunity to decline ~~registration~~Registration; decline credential
2173 provisioning; decline the presentation of their credentials; and decline release of their
2174 attributes or claims.

2175

2176 PRIVACY-11. OPTIONAL INFORMATION

2177 Entities MUST clearly indicate to USERS what personal information is mandatory and what
2178 information is optional prior to the transaction.

2179

2180 PRIVACY-12. ANONYMITY

2181 Wherever feasible, entities MUST utilize identity systems and processes that enable
2182 transactions that are anonymous, anonymous with validated attributes, pseudonymous, or
2183 where appropriate, uniquely identified. Where applicable to such transactions, entities
2184 employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES
2185 collecting USER personal information. Organizations MUST request individuals' credentials only
2186 when necessary for the transaction and then only as appropriate to the risk associated with the
2187 transaction or only as appropriate to the risks to the parties associated with the transaction.

2188

2189 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

2190 Controls on the processing or use of USERS' personal information MUST be commensurate with
2191 the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by
2192 entities who conduct digital identity management functions, to establish what risks those
2193 functions pose to USERS' privacy.

2194

2195 PRIVACY-14. DATA RETENTION AND DISPOSAL

2196 Entities MUST limit the retention of personal information to the time necessary for providing
2197 and administering the functions and services to USERS for which the information was collected,
2198 except as otherwise required by law or regulation. When no longer needed, personal
2199 information MUST be securely disposed of in a manner aligning with appropriate industry
2200 standards and/or legal requirements.

2201

2202 PRIVACY-15. ATTRIBUTE SEGREGATION

2203 Wherever feasible, identifier data MUST be segregated from attribute data.
2204 SECURE-1. SECURITY PRACTICES
2205 Entities MUST apply appropriate and industry-accepted information security STANDARDS,
2206 guidelines, and practices to the systems that support their identity functions and services.
2207
2208 SECURE-2. DATA INTEGRITY
2209 Entities MUST implement industry-accepted practices to protect the confidentiality and
2210 integrity of identity data—including authentication data and attribute values—during the
2211 execution of all digital identity management functions, and across the entire data lifecycle
2212 (collection through destruction).
2213
2214 SECURE-3. CREDENTIAL REPRODUCTION
2215 Entities that issue or manage credentials and tokens MUST implement industry-accepted
2216 processes to protect against their unauthorized disclosure and reproduction.
2217
2218 SECURE-4. CREDENTIAL PROTECTION
2219 Entities that issue or manage credentials and tokens MUST implement industry-accepted data
2220 integrity practices to enable individuals and other entities to verify the source of credential and
2221 token data.
2222
2223 SECURE-5. CREDENTIAL ISSUANCE
2224 Entities that issue or manage credentials and tokens MUST do so in a manner designed to
2225 assure that they are granted to the appropriate and intended USER(s) only. Where
2226 ~~registration~~Registration and credential issuance are executed by separate entities, procedures
2227 for ensuring accurate exchange of ~~registration~~Registration and issuance information that are
2228 commensurate with the stated assurance level MUST be included in business agreements and
2229 operating policies.
2230
2231 SECURE-6. CREDENTIAL UNIQUENESS
2232 Entities that issue or manage credentials MUST ensure that each account to credential pairing is
2233 uniquely identifiable within its namespace for authentication purposes.
2234
2235 SECURE-7. TOKEN CONTROL
2236 Entities that authenticate a USER MUST employ industry-accepted secure authentication
2237 protocols to demonstrate the USER's control of a valid token.
2238
2239 SECURE-8. MULTIFACTOR AUTHENTICATION
2240 Entities that authenticate a USER MUST offer authentication mechanisms which augment or are
2241 alternatives to a password.
2242
2243 SECURE-9. AUTHENTICATION RISK ASSESSMENT
2244 Entities MUST have a risk assessment process in place for the selection of authentication
2245 mechanisms and supporting processes.
2246

2247
2248
2249 SECURE-10. UPTIME
2250 Entities that provide and conduct digital identity management functions MUST have established
2251 policies and processes in place to maintain their stated assurances for availability of their
2252 services.
2253
2254 SECURE-11. KEY MANAGEMENT
2255 Entities that use cryptographic solutions as part of identity management MUST implement key
2256 management policies and processes that are consistent with industry-accepted practices.
2257
2258 SECURE-12. RECOVERY AND REISSUANCE
2259 Entities that issue credentials and tokens MUST implement methods for reissuance, updating,
2260 and recovery of credentials and tokens that preserve the security and assurance of the original
2261 ~~registration~~Registration and credentialing operations.
2262
2263 SECURE-13. REVOCATION
2264 Entities that issue credentials or tokens MUST have processes and procedures in place to
2265 invalidate credentials and tokens.
2266
2267 SECURE-14. SECURITY LOGS
2268 Entities conducting digital identity management functions MUST log their transactions and
2269 security events, in a manner that supports system audits and, where necessary, security
2270 investigations and regulatory requirements. Timestamp synchronization and detail of logs
2271 MUST be appropriate to the level of risk associated with the environment and transactions.
2272
2273 SECURE-15. SECURITY AUDITS
2274 Entities MUST conduct regular audits of their compliance with their own information security
2275 policies and procedures, and any additional requirements of law, including a review of their
2276 logs, incident reports and credential loss occurrences, and MUST periodically review the
2277 effectiveness of their policies and procedures in light of that data.
2278

DRAFT

2280

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

2282