

# COMMONWEALTH OF VIRGINIA



## Information Technology Resource Management (ITRM)

### GUIDANCE DOCUMENT

[Federation and Participant Requirements](#) ~~Electronic Authentication~~

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 .....	<a href="#">1415</a>
6	Minimum Specifications .....	<a href="#">1516</a>
7	<del>Alignment Comparison .....</del>	<del>26</del>

DRAFT

# 1 Publication Version Control

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

Publication Version	Date	Revision Description
1.0	<a href="#">07/2010/12/2016</a>	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 Federation and Participant Requirements in 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  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108

**Governing Statutes:**

**Secretary of Technology**

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

**Secretary of Transportation**

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

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

**Virginia Information Technologies Agency**

§ 2.2-2010. Additional powers of VITA  
<http://lis.virginia.gov/cgi-bin/legp604.exe?000+cod+2.2-2010>

**4 Definitions**

---

110  
111  
112

Terms used in this document comply with definitions in the Public Review version of the 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).<sup>1</sup>

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]<sup>2</sup> 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

---

<sup>1</sup> 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](http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf)

<sup>2</sup> [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. \[RFC 5280\]<sup>3</sup>](#)

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. \[GPG45\]<sup>4</sup>](#)

---

<sup>3</sup> [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>.

<sup>4</sup> [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.<sup>5</sup>  
311

---

<sup>5</sup> 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):<sup>6</sup>  
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.

<sup>6</sup> 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](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]<sup>7</sup> 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

<sup>7</sup> [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]<sup>8</sup>

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

---

<sup>8</sup> [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]<sup>9</sup>

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

---

<sup>9</sup> [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 **Digital Signature:** An asymmetric key operation where the private key is used to digitally sign  
755 data and the public key is used to verify the signature. Digital signatures provide authenticity  
756 protection, integrity protection, and non-repudiation.

757  
758 **Eavesdropping Attack:** An attack in which an attacker listens passively to the authentication  
759 protocol to capture information which can be used in a subsequent active attack to  
760 masquerade as the claimant.

761  
762 **Electronic Authentication:** The process of establishing confidence in user identities  
763 electronically presented to an information system.

764  
765 **Entropy:** A measure of the amount of uncertainty that an attacker faces to determine the value  
766 of a secret. Entropy is usually stated in bits.

767  
768 **Extensible Mark-up Language (XML):** Extensible Markup Language, abbreviated XML, describes  
769 a class of data objects called XML documents and partially describes the behavior of computer  
770 programs which process them.

771  
772 **Federal Bridge Certification Authority (FBCA):** The FBCA is the entity operated by the Federal  
773 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI  
774 Policy Authority to create, sign, and issue public key certificates to Principal CAs.

775

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.<sup>40</sup>

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

---

<sup>40</sup> 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~~ [Participants](#) 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 Federation and~~  
1079 ~~Participant Requirements authentication within an identity management system~~ [a Digital](#)  
1080 [Identity System](#). ~~The document assumes that the identity management system will be~~  
1081 ~~supported by a trust framework, compliant with Applicable Law.~~<sup>44</sup> The minimum specifications  
1082 have been ~~stated based on language in~~ [designed to be conformant with](#) NIST SP 800-63C-~~3~~.  
1083

<sup>44</sup> ~~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 governance models, minimum requirements processes, assurance levels,  
 1085 and Participant Requirements for a Federated Digital Identity System, components, process  
 1086 flows, assurance levels and privacy and security provisions for electronic authentication. The  
 1087 document assumes that specific business, legal and technical requirements for electronic  
 1088 authentication Participant Requirements will be established in the Trust Framework Identity  
 1089 Trust Framework for each distinct identity management system Digital Identity System, and that  
 1090 these requirements will be designed based on the Electronic Authentication model and  
 1091 Federation Identity Assurance Level (IALFAL) requirements) and Authenticator Assurance Level  
 1092 (AAL) requirements for the system.

1094 The document limits its focus to electronic authentication Federation and Participant  
 1095 Requirements. Minimum specifications for other components of an identity management  
 1096 system a Digital Identity System will have been defined in separate IMSAC guidance  
 1097 documents in this series, pursuant to §2.2-436 and §2.2-437.

## 1099 6 Minimum Specifications

1100 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3)  
 1101 defines an “electronic authentication Federation” in a Digital Identity System as “A process that  
 1102 allows for the conveyance of identity and authentication information across a set of networked  
 1103 systems the process of establishing confidence in the identity of users or information  
 1104 systems.”<sup>12</sup> Information systems may use the authenticated identity to determine if that user is  
 1105 authorized to perform an electronic transaction. Federation of a Digital Identity System  
 1106 depends upon each member, or Participant, in the system complying with Participant  
 1107 Requirements, the set of rules and policies assigned to each member type by the system’s  
 1108 Identity Trust Framework.

1111 This document establishes minimum specifications for electronic authentication Federation and  
 1112 Participant Requirements in a Digital Identity System conformant with and using language  
 1113 from NIST SP 800-63-3. However, the minimum specifications defined in this document have  
 1114 been developed to accommodate requirements for electronic authentication Federation and  
 1115 Participant Requirements established under other national and international standards.<sup>13</sup> The  
 1116 minimum specifications in this document also assume that specific business, legal and technical  
 1117 requirements for an identity management system will be documented in the trust framework

<sup>12</sup> 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.

<sup>13</sup> 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](http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf) 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 ~~for that system.~~ Minimum specifications for other components of ~~an identity management~~  
 1119 ~~system~~ a Digital Identity System have been documented in separate guidance documents in the  
 1120 IMSAC series, pursuant to §2.2-436 and §2.2-437.

1121

## 1122 Electronic Authentication Model

1123

1124 Electronic ~~authentication~~ Authentication is the process of establishing confidence in  
 1125 individual identities presented to a ~~digital system~~ Digital Identity System. In a Federated Digital  
 1126 Identity Systems, Electronic Authentication and related flows of identity information occur  
 1127 across a set of network systems. These systems are often run and controlled by disparate  
 1128 members in different network and security domains can use the authenticated identity to  
 1129 determine if that individual is authorized to perform an online transaction. The minimum  
 1130 specifications in this document assume that the authentication and transaction take place  
 1131 across a network. Therefore, Federation requires Electronic Authentication models to be  
 1132 extended to take into account the roles played by each member type and the corresponding  
 1133 Participant Requirements.

1134

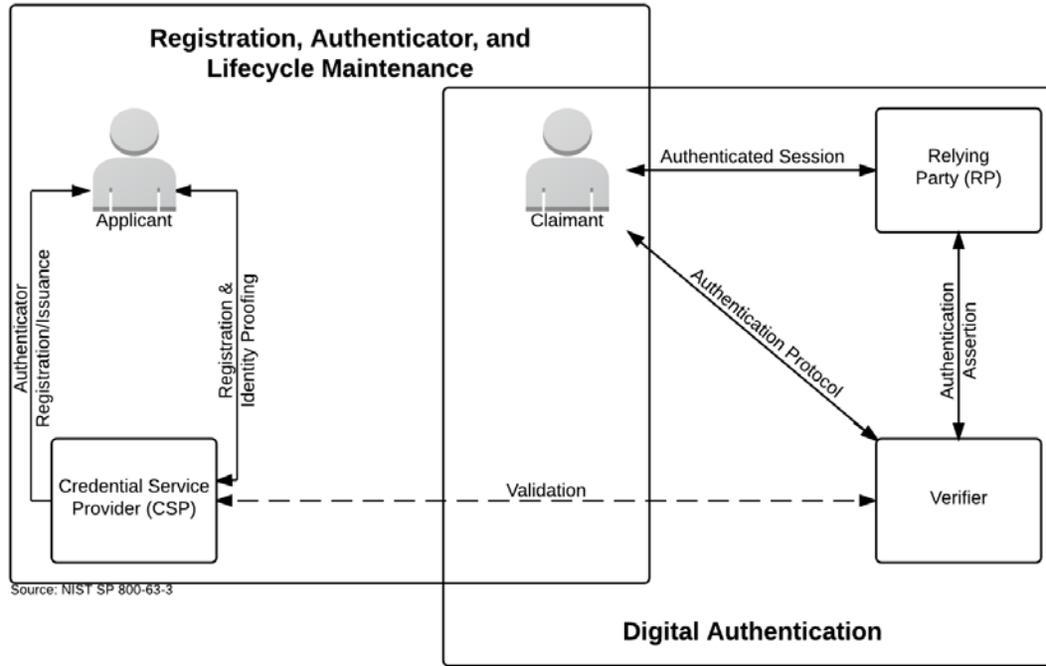
1135 ~~The electronic authentication model~~ The minimum specifications for Federation and Participant  
 1136 Requirements defined in this document reflect the Electronic Authentication model defined in  
 1137 these minimum specifications reflects current technologies and architectures used primarily by  
 1138 governmental entities. More complex models that separate functions among a broader range  
 1139 of ~~parties~~ Participants are also available and may have advantages in some classes of  
 1140 applications. While a simpler model ~~has been defined in~~ serves as the basis for these minimum  
 1141 specifications, it does not preclude ~~participant member~~ in ~~identity management system~~ Digital  
 1142 Identity Systems from separating these functions. Minimum specifications for the Electronic  
 1143 Authentication model reflected in this document have been defined in ITRM Guidance  
 1144 Document: Electronic Authentication, and a graphic of the model has been shown in Figure 1.

Formatted: Font: Italic

Formatted: Font: Bold

1145

**Figure 1. Electronic Authentication Model**



1146

1147

1148

1149

1150

1151

1152

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

1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163

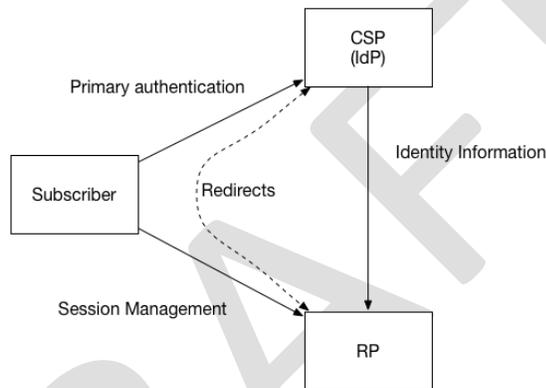
## Federation

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

Formatted: Font: Bold

**Figure 2: Federation Model**

Formatted: Font: Bold



Formatted: Font: Bold

Formatted: Centered

Formatted: Font: Bold

1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182

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

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

Formatted: Font: Italic

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

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

1183 [capabilities for Subscriber tracking and use of profile information that do not align with the](#)  
1184 [privacy interests of the Subscribers.](#)

1185  
1186 [The IdP must not disclose information on Subscriber activities at an RP to any Participant, nor](#)  
1187 [use the information for any purpose other than Federated authentication, to comply with law](#)  
1188 [or legal process, or in the case of a specific user request for the information. The IdP SHOULD](#)  
1189 [employ technical measures to provide unlinkability and prevent Subscriber activity tracking and](#)  
1190 [profiling. A IdP may disclose information on Subscriber activities to other RPs within the](#)  
1191 [Federation for security purposes such as communication of compromised Subscriber accounts.](#)

## 1192 1193 [Federation Models](#)

Formatted: Font: 13 pt

1195 [This section provides an overview of a few common models of identity Federation currently in](#)  
1196 [use. In these models, a relationship is established between Participants of the Federation in](#)  
1197 [several different ways. Some models mandate that all Federated Participants have an equally](#)  
1198 [high level of trust, while other models allow for Participants with a diversity of relationships.](#)

### 1199 [Central Authority](#)

1201 [Some Federated Participants defer to a central authority to make decisions for them and to](#)  
1202 [communicate metadata between Participants. In this model, the central authority generally](#)  
1203 [conducts some level of vetting on each Participant in the Federation to verify compliance with](#)  
1204 [predetermined security and integrity standards.](#)

1206 [Most Federations using the central authority model have a simple membership model - either](#)  
1207 [Participants are in the Federation or they are not. However, more sophisticated Federations](#)  
1208 [have multiple tiers of membership which can be used by Federated Participants to tell whether](#)  
1209 [other Participants in the Federation have been more thoroughly vetted or have some common](#)  
1210 [purpose that justifies a higher level of access. As a consequence, some Participants in the](#)  
1211 [Federation are more likely to automatically release information about their Subscribers to the](#)  
1212 [Participants in the higher tiers.](#)

### 1213 [Manual Registration](#)

1215 [In the manual registration model of Federation, system administrators communicate metadata](#)  
1216 [and test system interoperability before transactions take place between users over the wire.](#)  
1217 [Metadata for each Participant who wishes to participate is manually input into a registry of](#)  
1218 [Federated Participants. Each Participant maintains their own registry of other Participants with](#)  
1219 [whom they wish to federate.](#)

1221 [Manual registration can take place on a case by case basis without any authority or Federation](#)  
1222 [operator in place. In this case, a pairwise relationship is created between the IdP and the RP.](#)

1224 [Manual registration can also work in concert with a central authority model. In this case, a](#)  
1225 [registry is pre-populated with Participants known to the central authority, and more](#)  
1226 [Participants are added manually on an as-needed basis.](#)

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

1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266

### Dynamic Registration

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

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

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

### Proxied Federation

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

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

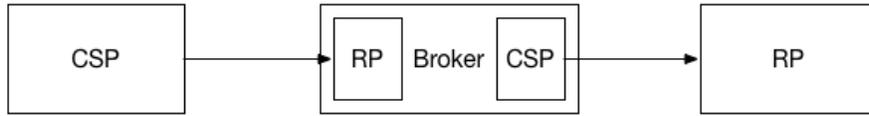
Formatted: Font: Bold

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

1267

**Figure 3: Federation Proxy Model**

Formatted: Font: Bold



1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

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

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

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

1288

The following list documents a spectrum of blinding implementations:

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

1302

1303

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

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

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

1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346

Runtime Decisions

Formatted: Font: 13 pt

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

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

Federation Assurance Level

Formatted: Font: 13 pt

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

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

Examples of Assertions Protocols:

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

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

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

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

Formatted: Font: Bold

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

1347

1348

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

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

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

1349

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

1350

1351

1352

1353

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

1354

1355

1356

1357

1358

1359

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

1360

1361

1362

1363

1364

1365

**Participant Requirements**

1366

1367

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

1368

1369

1370

1371

1372

1373

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

1374

1375

1376

1377

1378

1379

Formatted: Font: Italic

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

1380 Registration Authorities (RAs)  
 1381 RAs establish and vouch for the Identity or Attributes of an Applicant to a CSP. RAs may be an  
 1382 integral part of a CSP, or it may be independent of a CSP, but it maintains a trusted relationship  
 1383 to the CSP(s). Primary requirements for RAs include the following:

- 1384 • Perform Physical or Virtual In-Person Proofing functions on identity evidence submitted  
 1385 by an Applicant for a Claimed Identity
- 1386 • Verify and validate identity evidence submitted by an Applicant to support a Claimed  
 1387 Identity during a Registration event.
- 1388 • Perform Registration (or enrollment) of Applicants for which the Claimed Identity has  
 1389 been verified, validated, and accepted
- 1390 • Issue an appropriate Credential to a registered Subscriber who has completed the  
 1391 Registration process
- 1392 • Manage, monitor, and audit the usage of Credentials by Subscribers who have  
 1393 Registered with the RA
- 1394 • Establish and implement a process to revoke a Subscriber’s Credential in the event of  
 1395 improper use, irregularities, or a security breach
- 1396 • Manage required post-issuance updates or modifications to a Subscriber’s Credential  
 1397 based on verified and validated changes in the Claimed Identity or identity evidence
- 1398 • Establish and implement a process to re-issue a Subscriber’s Credential when corrective  
 1399 action has been taken or the identity evidence has been updated

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

1400 Identity Providers (IdPs)  
 1401 IdPs manage the Subscriber’s primary authentication Credentials and issue Assertions derived  
 1402 from those Credentials, generally to the CSP. Primary requirements for IdPs include the  
 1403 following:

- 1405 • Provide a trust model that ensures that an individual is linked to identities which have  
 1406 been issued, protected, and managed to provide the accuracy of asserted Attributes
- 1407 • Develop and provide an Authentication process by which the user (Subscriber or  
 1408 Applicant) provides evidence to the IdP, who independently verifies that the user is who  
 1409 he or she claims to be
- 1410 • Develop a process to periodically reevaluate the status of the user and the validity of his  
 1411 or her associated Identity
- 1412 • Develop a process for Attribute management to ensure the timely cancellation or  
 1413 modification of Attributes should the user’s status change
- 1414 • Develop a process for auditing the Attribute identification process, including registration  
 1415 activities, to ensure Attributes are maintained in accordance with the process specified  
 1416 by that IdP
- 1417 • Conduct audit functions in a manner to identify any irregularities or security breaches
- 1418 • Provide to the Federation audit information, upon request
- 1419 • Provide a process to assist users who have either lost or forgotten their means of  
 1420 Authentication

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

1421  
 1422

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

1423 Credential Service Providers (CSPs)  
 1424 CSPs issue or register Subscriber authenticators and issue electronic credentials to Subscribers.  
 1425 The CSP may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may  
 1426 be an independent third party, or may issue credentials for its own use. Primary requirements  
 1427 for CSPs include the following:

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

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

1433 Verifiers  
 1434 Verifiers confirm the Claimant’s Identity by verifying the Claimant’s possession and control of  
 1435 one or more Authenticators using an authentication protocol. Primary requirements for  
 1436 Verifiers include the following:

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

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

1443 Relying Parties  
 1444 RPs accept the Subscriber’s Authenticator(s) and Credentials or a Verifier’s Assertion of a  
 1445 Claimant’s Identity, typically to process a transaction or grant access to information, network,  
 1446 or Information System. Primary requirements for RPs include the following:

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

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

1454

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

1455 In addition, certain registration, identity proofing, and issuance processes performed by the  
1456 credential service provider (CSP) may be delegated to an entity known as the registration  
1457 authority (RA) or identity manager (IM). A close relationship between the RA/IM and CSP is  
1458 typical, and the nature of this relationship may differ among RAs, IMs, and CSPs. The minimum  
1459 specifications defined in this document assume that relationships between participants and  
1460 their requirements are established in the trust framework for the identity management system.

1461  
1462 Electronic authentication begins with registration (also referred to as enrollment). The usual  
1463 sequence for registration proceeds as follows. An applicant applies to a CSP. If approved, the  
1464 CSP creates a credential and binds it to one or more authenticators. The credential includes an  
1465 identifier, which can be pseudonymous, and one or more attributes that the CSP has verified.  
1466 The authenticators may be issued by the CSP, generated/provided directly by the subscriber, or  
1467 provided by a third party. The authenticator and credential may be used in subsequent  
1468 authentication events.

1469  
1470 The process used to verify an applicant's association with their real world identity is called  
1471 identity proofing. The strength of identity proofing is described by a categorization called the  
1472 identity assurance level (IAL, see subsection on Assurance Level Model below in this document).  
1473 Minimum specifications for identity proofing and verification during the registration process  
1474 have been established in *ITRM Guidance Document: Identity Proofing and Verification*.

1475  
1476 At IAL 1, identity proofing is not required, therefore any attribute information provided by the  
1477 subscriber is self-asserted and not verified. At IAL 2 and 3, identity proofing is required, but the  
1478 CSP may assert verified attribute values, verified attribute claims, pseudonymous identifiers, or  
1479 nothing. This information assists Relying Parties (RPs) in making access control or authorization  
1480 decisions. RPs may decide that their required IAL is 2 or 3, but may only need specific  
1481 attributes, and perhaps attributes that retain an individual's pseudonymity. A relying party may  
1482 also employ a federated identity approach where the RP outsources all identity proofing,  
1483 attribute collection, and attribute storage to a CSP.

1484  
1485 In these minimum specifications, the party to be authenticated is called a claimant and the  
1486 party verifying that identity is called a verifier. When a claimant successfully demonstrates  
1487 possession and control of one or more authenticators to a verifier through an authentication  
1488 protocol, the verifier can verify that the claimant is a valid subscriber. The verifier passes on an  
1489 assertion about the subscriber, who may be either pseudonymous or non-pseudonymous, to  
1490 the RP. That assertion includes an identifier, and may include identity information about the  
1491 subscriber, such as the name, or other attributes that were verified in the enrollment process  
1492 (subject to the policies of the CSP and the trust framework for the system). When the verifier is  
1493 also the RP, the assertion may be implicit. The RP can use the authenticated information  
1494 provided by the verifier to make access control or authorization decisions.

1495  
1496 Authentication establishes confidence in the claimant's identity, and in some cases in the  
1497 claimant's attributes. Authentication does not determine the claimant's authorizations or  
1498 access privileges; this is a separate decision. RPs will use a subscriber's authenticated identity

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

1499 and attributes with other factors to make access control or authorization decisions. Nothing in  
1500 this document precludes RPs from requesting additional information from a subscriber that has  
1501 successfully authenticated.

1502  
1503 The strength of the authentication process is described by a categorization called the  
1504 authenticator assurance level (AAL). AAL 1 requires single-factor authentication and is  
1505 permitted with a variety of different authenticator types. At AAL 2, authentication requires two  
1506 authentication factors for additional security. Authentication at the highest level, AAL 3,  
1507 requires the use of a hardware-based authenticator and one other factor.

1508  
1509 As part of authentication, mechanisms such as device identity or geo-location may be used to  
1510 identify or prevent possible authentication false positives. While these mechanisms do not  
1511 directly increase the authenticator assurance level, they can enforce security policies and  
1512 mitigate risks. In many cases, the authentication process and services will be shared by many  
1513 applications and agencies. However, it is the individual agency or application acting as the RP  
1514 that shall make the decision to grant access or process a transaction based on the specific  
1515 application requirements.

#### 1516 Authentication Components and Process Flows

Formatted: Font: 12 pt

1517  
1518  
1519 The various entities and interactions that comprise the electronic authentication model defined  
1520 in these minimum specifications have been illustrated below in **Figure 1**. The left shows the  
1521 enrollment, credential issuance, lifecycle management activities, and the stages an individual  
1522 transitions, based on the specific phase of the identity proofing and authentication process.

1523  
1524 The authentication process begins with the claimant demonstrating to the verifier possession  
1525 and control of an authenticator that is bound to the asserted identity through an authentication  
1526 protocol. Once possession and control have been demonstrated, the verifier confirms that the  
1527 credential remains valid, usually by interacting with the CSP.

1528  
1529 The exact nature of the interaction between the verifier and the claimant during the  
1530 authentication protocol contributes to the overall security of the system. Well-designed  
1531 protocols can protect the integrity and confidentiality of traffic between the claimant and the  
1532 verifier both during and after the authentication exchange, and it can help limit the damage  
1533 that can be done by an attacker masquerading as a legitimate verifier.

1534  
1535 Additionally, mechanisms located at the verifier can mitigate online guessing attacks against  
1536 lower entropy secrets like passwords and PINs by limiting the rate at which an attacker can  
1537 make authentication attempts or otherwise delaying incorrect attempts. Generally, this is done  
1538 by keeping track of and limiting the number of unsuccessful attempts, since the premise of an  
1539 online guessing attack is that most attempts will fail.

1540  
1541 The verifier is a functional role, but is frequently implemented in combination with the CSP  
1542 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

1543 that the verifier does not learn the subscriber's authenticator secret in the process of  
1544 authentication, or at least to ensure that the verifier does not have unrestricted access to  
1545 secrets stored by the CSP.  
1546

1547 The usual sequence of interactions in the authentication process is as follows:

- 1548 1. An applicant applies to a CSP through a registration process.
- 1549 2. The CSP identity proofs that applicant. Upon successful proofing, the applicant becomes  
1550 a subscriber.
- 1551 3. An authenticator and a corresponding credential are established between the CSP and  
1552 the new subscriber.
- 1553 4. The CSP maintains the credential, its status, and the enrollment data collected for the  
1554 lifetime of the credential. The subscriber maintains his or her authenticator.  
1555

1556 Other sequences are less common, but could also achieve the same functional requirements.  
1557 The right side of Figure 1 shows the entities and the interactions related to using an  
1558 authenticator to perform electronic authentication. When the subscriber needs to authenticate  
1559 to perform a transaction, he or she becomes a claimant to a verifier. The interactions are as  
1560 follows:

- 1561 1. The claimant proves to the verifier that he or she possesses and controls the  
1562 authenticator through an authentication protocol.
- 1563 2. The verifier interacts with the CSP to validate the credential that binds the subscriber's  
1564 identity to his or her authenticator and to optionally obtain claimant attributes.
- 1565 3. If the verifier is separate from the RP (application), the verifier provides an assertion  
1566 about the subscriber to the RP, which may use the information in the assertion to make  
1567 an access control or authorization decision.
- 1568 4. An authenticated session is established between the subscriber and the RP.  
1569

1570 In all cases, the RP should request the attributes it requires from a CSP prior to authentication  
1571 of the claimant. In addition, the claimant should be requested to consent to the release of  
1572 those attributes prior to generation and release of an assertion.  
1573

1574 In some cases, the verifier does not need to communicate in real time with the CSP to complete  
1575 the authentication activity (e.g., some uses of digital certificates). Therefore, the dashed line  
1576 between the verifier and the CSP represents a logical link between the two entities rather than  
1577 a physical link. In some implementations, the verifier, RP and the CSP functions may be  
1578 distributed and separated as shown in Figure 1; however, if these functions reside on the same  
1579 platform, the interactions between the components are local messages between applications  
1580 running on the same system rather than protocols over shared untrusted networks.  
1581

1582 As noted above, CSPs maintain status information about issued credentials. CSPs may assign a  
1583 finite lifetime to a credential in order to limit the maintenance period. When the status  
1584 changes, or when the credentials near expiration, credentials may be renewed or re-issued; or,  
1585 the credential may be revoked or destroyed. Typically, the subscriber authenticates to the CSP  
1586 using his or her existing, unexpired authenticator and credential in order to request issuance of

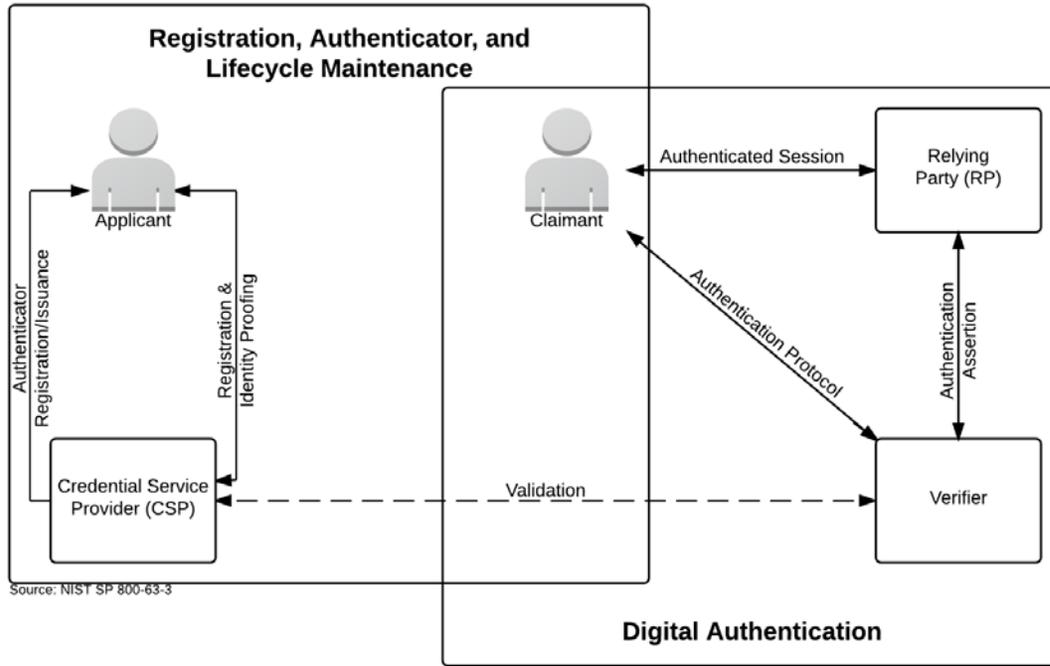
Formatted: Position: Vertical: -0.04", Relative to: Paragraph

1587 a new authenticator and credential. If the subscriber fails to request authenticator and  
1588 credential re-issuance prior to their expiration or revocation, he or she may be required to  
1589 repeat the enrollment process to obtain a new authenticator and credential. Alternatively, the  
1590 CSP may choose to accept a request during a grace period after expiration.

DRAFT

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

1591 **Figure 1. Electronic Authentication Model**



1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600

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

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

Formatted: Font: 12 pt  
Formatted: Default Paragraph Font, Font: 12 pt

1601 Authentication Protocols and Lifecycle Management

1602  
1603 Authenticators

1604 The established paradigm for electronic authentication identifies three factors as the  
1605 cornerstone of authentication:

- 1606     ■ Something you know (for example, a password)
- 1607     ■ Something you have (for example, an ID badge or a cryptographic key)
- 1608     ■ Something you are (for example, a fingerprint or other biometric data)

1609  
1610 Multi-factor authentication refers to the use of more than one of the factors listed above. The  
1611 strength of authentication systems is largely determined by the number of factors incorporated  
1612 by the system. Implementations that use two different factors are considered to be stronger  
1613 than those that use only one factor; systems that incorporate all three factors are stronger than  
1614 systems that only incorporate two of the factors. Other types of information, such as location  
1615 data or device identity, may be used by an RP or verifier to evaluate the risk in a claimed  
1616 identity, but they are not considered authentication factors.

1617  
1618 In electronic authentication the claimant possesses and controls one or more authenticators  
1619 that have been registered with the CSP and are used to prove the claimant's identity. The  
1620 authenticator(s) contains secrets the claimant can use to prove that he or she is a valid  
1621 subscriber, the claimant authenticates to a system or application over a network by proving  
1622 that he or she has possession and control of an authenticator.

1623  
1624 The secrets contained in authenticators are based on either public key pairs (asymmetric keys)  
1625 or shared secrets (symmetric keys). A public key and a related private key comprise a public key  
1626 pair. The private key is stored on the authenticator and is used by the claimant to prove  
1627 possession and control of the authenticator. A verifier, knowing the claimant's public key  
1628 through some credential (typically a public key certificate), can use an authentication protocol  
1629 to verify the claimant's identity, by proving that the claimant has possession and control of the  
1630 associated private key authenticator.

1631  
1632 Shared secrets stored on authenticators may be either symmetric keys or passwords. While  
1633 they can be used in similar protocols, one important difference between the two is how they  
1634 relate to the subscriber. While symmetric keys are generally stored in hardware or software  
1635 that the subscriber controls, passwords are intended to be memorized by the subscriber. As  
1636 such, keys are something the subscriber has, while passwords are something he or she knows.  
1637 Since passwords are committed to memory, they usually do not have as many possible values  
1638 as cryptographic keys, and, in many protocols, are severely vulnerable to network attacks that  
1639 are more restricted for keys.

1640  
1641 Moreover, the entry of passwords into systems (usually through a keyboard) presents the  
1642 opportunity for very simple keyboard logging attacks, and may also allow those nearby to learn  
1643 the password by watching it being entered. Therefore, keys and passwords demonstrate  
1644 somewhat separate authentication properties (something you have rather than something you

1645 know). When using either public key pairs or shared secrets, the subscriber has a duty to  
1646 maintain exclusive control of his or her authenticator, since possession and control of the  
1647 authenticator is used to authenticate the claimant's identity.

1648  
1649 The minimum specifications defined in this document assume that authenticators always  
1650 contain a secret. Authentication factors classified as something you know are not necessarily  
1651 secrets. Knowledge-based authentication, where the claimant is prompted to answer questions  
1652 that can be confirmed from public databases, also does not constitute an acceptable secret for  
1653 electronic authentication. More generally, something you are does not generally constitute a  
1654 secret. However, the requirements for some identity management systems may allow the use  
1655 of biometrics as an authenticator.

1656  
1657 Biometric characteristics are unique personal attributes that can be used to verify the identity  
1658 of a person who is physically present at the point of verification. They include facial features,  
1659 fingerprints, iris patterns, voiceprints, and many other characteristics. NIST recommends that  
1660 biometrics be used in the enrollment process for higher levels of assurance to later help  
1661 prevent a subscriber who is registered from repudiating the enrollment, to help identify those  
1662 who commit enrollment fraud, and to unlock authenticators. The specific requirements for the  
1663 use of biometrics must be defined in the trust framework for the system.

1664  
1665 The minimum specifications in this document encourage identity management systems to use  
1666 authentication processes and protocols that incorporate all three factors, as a means of  
1667 enhancing system security. An electronic authentication system may incorporate multiple  
1668 factors in either of two ways. The system may be implemented so that multiple factors are  
1669 presented to the verifier, or some factors may be used to protect a secret presented to the  
1670 verifier. If multiple factors are presented to the verifier, each will need to be an authenticator  
1671 (and therefore contain a secret). If a single factor is presented to the verifier, the additional  
1672 factors are used to protect the authenticator and need not themselves be authenticators.

#### 1673 1674 Credentials

1675 As described in the preceding sections, credentials bind an authenticator to the subscriber as  
1676 part of the issuance process. Credentials are stored and maintained by the CSP. The claimant  
1677 possesses an authenticator, but is not necessarily in possession of the electronic credentials.  
1678 For example, database entries containing the user attributes are considered to be credentials  
1679 for the purpose of this document but are possessed by the verifier.

#### 1680 1681 Assertions

1682 Upon completion of the electronic authentication process, the verifier generates an assertion  
1683 containing the result of the authentication and provides it to the RP. If the verifier is  
1684 implemented in combination with the RP, the assertion is implicit. If the verifier is a separate  
1685 entity from the RP, as in typical federated identity models, the assertion is used to  
1686 communicate the result of the authentication process, and optionally information about the  
1687 subscriber, from the verifier to the RP.

1688 Assertions may be communicated directly to the RP, or can be forwarded through the  
 1689 subscriber, which has further implications for system design. An RP trusts an assertion based  
 1690 on the source, the time of creation, and the corresponding trust framework that governs the  
 1691 policies and process of CSPs and RPs. The verifier is responsible for providing a mechanism by  
 1692 which the integrity of the assertion can be confirmed.

1693  
 1694 The RP is responsible for authenticating the source (e.g., the verifier) and for confirming the  
 1695 integrity of the assertion. When the verifier passes the assertion through the subscriber, the  
 1696 verifier must protect the integrity of the assertion in such a way that it cannot be modified by  
 1697 the subscriber. However, if the verifier and the RP communicate directly, a protected session  
 1698 may be used to provide the integrity protection. When sending assertions across a network, the  
 1699 verifier is responsible for ensuring that any sensitive subscriber information contained in the  
 1700 assertion can only be extracted by an RP that it trusts to maintain the information's  
 1701 confidentiality.

1702  
 1703 Examples of assertions include:

- 1704 • SAML Assertions — SAML assertions are specified using a mark-up language intended for  
 1705 describing security assertions. They can be used by a verifier to make a statement to an  
 1706 RP about the identity of a claimant. SAML assertions may be digitally signed.
- 1707 • OpenID Connect Claims — OpenID Connect are specified using JavaScript Object Notation  
 1708 (JSON) for describing security, and optionally, user claims. JSON user info claims may be  
 1709 digitally signed.
- 1710 • Kerberos Tickets — Kerberos Tickets allow a ticket granting authority to issue session  
 1711 keys to two authenticated parties using symmetric key based encapsulation schemes.

1712  
 1713 **Relying Parties**

1714 An RP relies on results of an authentication protocol to establish confidence in the identity or  
 1715 attributes of a subscriber for the purpose of conducting an online transaction. RPs may use a  
 1716 subscriber's authenticated identity (pseudonymous or non-pseudonymous), the IAL, AAL, and  
 1717 other factors to make access control or authorization decisions. The verifier and the RP may be  
 1718 the same entity, or they may be separate entities. If they are separate entities, the RP normally  
 1719 receives an assertion from the verifier. The RP ensures that the assertion came from a verifier  
 1720 trusted by the RP. The RP also processes any additional information in the assertion, such as  
 1721 personal attributes or expiration times.

1722  
 1723

Formatted: Font: 12 pt, Not Bold

Formatted: Font: Not Bold

Formatted: Font: 12 pt, Not Bold

1724 Assurance Model

Formatted: Font: Not Bold

Formatted: Normal

1725  
1726 The minimum specifications defined in this document for electronic authentication assume that  
1727 the trust framework for an identity management system will define a specific assurance model  
1728 for that system.<sup>44</sup> Therefore, the assurance model presented below, which is based on NIST SP  
1729 800-63-3, should be viewed as a recommended framework for electronic authentication. Other  
1730 assurance models have been established in OMB M-04-04 and the State Identity, Credential,  
1731 and Access Management (SICAM) guidelines, published by the National Association of Chief  
1732 Information Officers (NASCIO). A crosswalk showing disparities in the NIST SP 800-63-3, OMB  
1733 M-04-04, and SICAM assurance models has been provided in **Figure 2**.

1734  
1735 **Identity Assurance Level 1**—At this level, attributes provided in conjunction with the  
1736 authentication process, if any, are self-asserted.

1737  
1738 **Identity Assurance Level 2**—IAL 2 introduces the need for either remote or in-person identity  
1739 proofing. IAL 2 requires identifying attributes to have been verified in-person or remotely using,  
1740 at a minimum, the procedures given in NIST 800-63A.

1741  
1742 **Identity Assurance Level 3**—At IAL 3, in-person identity proofing is required. Identifying  
1743 attributes must be verified by an authorized representative of the CSP through examination of  
1744 physical documentation as described in NIST 800-63A.

1745  
1746 **Authenticator Assurance Level 1**—AAL 1 provides single factor electronic authentication, giving  
1747 some assurance that the same claimant who participated in previous transactions is accessing  
1748 the protected transaction or data. AAL 1 allows a wide range of available authentication  
1749 technologies to be employed and requires only a single authentication factor to be used. It also  
1750 permits the use of any of the authentication methods of higher authenticator assurance levels.  
1751 Successful authentication requires that the claimant prove through a secure authentication  
1752 protocol that he or she possesses and controls the authenticator.

1753  
1754 **Authenticator Assurance Level 2**—AAL 2 provides higher assurance that the same claimant who  
1755 participated in previous transactions is accessing the protected transaction or data. Two  
1756 different authentication factors are required. Various types of authenticators, including multi-  
1757 factor Software Cryptographic Authenticators, may be used as described in NIST 800-63B. AAL 2  
1758 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires  
1759 cryptographic mechanisms that protect the primary authenticator against compromise by the  
1760 protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved  
1761 cryptographic techniques are required for all assertion protocols used at AAL 2 and above.<sup>45</sup>

<sup>44</sup> 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.

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

1762 Authenticator Assurance Level 3 – AAL 3 is intended to provide the highest practical electronic  
 1763 authentication assurance. Authentication at AAL 3 is based on proof of possession of a key  
 1764 through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only “hard”  
 1765 cryptographic authenticators are allowed. The authenticator is required to be a hardware  
 1766 cryptographic module validated at Federal Information Processing Standard (FIPS) 140 Level 2  
 1767 or higher overall with at least FIPS 140 Level 3 physical security. AAL 3 authenticator  
 1768 requirements can be met by using the PIV authentication key of a FIPS 201 compliant Personal  
 1769 Identity Verification (PIV) Card.

1770 **Figure 2. Assurance Model Crosswalk**

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

Formatted: Font: 12 pt

1773

## 1774 Privacy and Security

1775

1776 The minimum specifications established in this document for privacy and security in the use of  
 1777 person information for ~~electronic authentication~~ [Electronic Authentication](#) apply the Fair  
 1778 Information Practice Principles (FIPPs).<sup>16</sup> The FIPPs have been endorsed by the National  
 1779 Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.<sup>17</sup>

1780

1781 The minimum specifications also adhere to the Identity Ecosystem Framework (IDEF) Baseline  
 1782 Functional Requirements (v.1.0) for privacy and security, adopted by the Identity Ecosystem  
 1783 Steering Group (IDESG) in October 2015 (**Appendix 2**).

1784

1785 The minimum specifications for ~~identity proofing~~ [Assertions and verification](#) apply the following  
 1786 FIPPs:

- 1787 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants  
 1788 regarding collection, use, dissemination, and maintenance of person information required  
 1789 during the ~~registration~~ [Registration](#), ~~identity proofing~~ [Identity Proofing](#) and verification  
 1790 processes.
- 1791 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using  
 1792 person information and, to the extent practicable, seek consent for the collection, use,  
 1793 dissemination, and maintenance of that information. RAs and CSPs also should provide  
 1794 mechanisms for appropriate access, correction, and redress of person information.
- 1795 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits  
 1796 the collection of person information and specifically articulate the purpose or purposes for  
 1797 which the information is intended to be used.
- 1798 • Data Minimization: RAs and CSPs should collect only the person information directly  
 1799 relevant and necessary to accomplish the ~~registration~~ [Registration](#) and related processes,  
 1800 and only retain that information for as long as necessary to fulfill the specified purpose.
- 1801 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for  
 1802 the purpose specified in the notice. Disclosure or sharing that information should be limited  
 1803 to the specific purpose for which the information was collected.
- 1804 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that  
 1805 person information is accurate, relevant, timely, and complete.
- 1806 • Security: RAs and CSPs should protect personal information through appropriate security  
 1807 safeguards against risks such as loss, unauthorized access or use, destruction, modification,  
 1808 or unintended or inappropriate disclosure.

<sup>16</sup> 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](#).

<sup>17</sup> 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>.

1809 Accountability and Auditing: RAs and CSPs should be accountable for complying with these  
 1810 principles, providing training to all employees and contractors who use person information,  
 1811 and auditing the actual use of person information to demonstrate compliance with these  
 1812 principles and all applicable privacy protection requirements.

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

1852  
1853  
1854  
1855

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

## 1856 Appendix 1. IMSAC Charter

1857

1858

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

1860

1861

1862

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

1863

1864

1865

1866

1867

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.

1868

1869

1870

1871

1872

1873

1874

1875

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

1876

1877

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

1878

1879

1880

1881

1882

1883

1884

1885

1886

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

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

1887

1888

1889

1890

1891

1892

1893

1894

1895

1896

1897

1898 The formation, membership and governance structure for the Advisory Council has been  
1899 codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

1900  
1901 The statutory authority and requirements for public notice and comment periods for guidance  
1902 documents have been established pursuant to § 2.2-437.C, as follows:

1903  
1904 C. Proposed guidance documents and general opportunity for oral or written submittals as to  
1905 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published  
1906 in the Virginia Register of Regulations as a general notice following the processes and  
1907 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§  
1908 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written  
1909 comments following the posting and publication and shall hold at least one meeting dedicated  
1910 to the receipt of oral comment no less than 15 days after the posting and publication. The  
1911 Advisory Council shall also develop methods for the identification and notification of interested  
1912 partiesParticipants and specific means of seeking input from interested persons and groups.  
1913 The Advisory Council shall send a copy of such notices, comments, and other background  
1914 material relative to the development of the recommended guidance documents to the Joint  
1915 Commission on Administrative Rules.

1916  
1917  
1918 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the  
1919 minutes of the meeting and related IMSAC documents, visit:  
1920 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

1921 Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline  
1922 Functional Requirements (v.1.0) for Privacy and Security

1923

1924 PRIVACY-1. DATA MINIMIZATION

1925 Entities MUST limit the collection, use, transmission and storage of personal information to the  
1926 minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities  
1927 providing claims or attributes MUST NOT provide any more personal information than what is  
1928 requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to  
1929 accommodate information requests of variable granularity, to support data minimization.

1930

1931 PRIVACY-2. PURPOSE LIMITATION

1932 Entities MUST limit the use of personal information that is collected, used, transmitted, or  
1933 stored to the specified purposes of that transaction. Persistent records of contracts, assurances,  
1934 consent, or legal authority MUST be established by entities collecting, generating, using,  
1935 transmitting, or storing personal information, so that the information, consistently is used in  
1936 the same manner originally specified and permitted.

1937

1938 PRIVACY-3. ATTRIBUTE MINIMIZATION

1939 Entities requesting attributes MUST evaluate the need to collect specific attributes in a  
1940 transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST  
1941 collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever  
1942 feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities  
1943 MUST be bound to claims instead of actual attribute values.

1944

1945 PRIVACY-4. CREDENTIAL LIMITATION

1946 Entities MUST NOT request USERS' credentials unless necessary for the transaction and then  
1947 only as appropriate to the risk associated with the transaction or to the risks to the  
1948 [parties](#) [Participants](#) associated with the transaction.

1949

1950 PRIVACY-5. DATA AGGREGATION RISK

1951 Entities MUST assess the privacy risk of aggregating personal information, in systems and  
1952 processes where it is collected, generated, used, transmitted, or stored, and wherever feasible,  
1953 MUST design and operate their systems and processes to minimize that risk. Entities MUST  
1954 assess and limit linkages of personal information across multiple transactions without the  
1955 USER's explicit consent.

1956

1957 PRIVACY-6. USAGE NOTICE

1958 Entities MUST provide concise, meaningful, and timely communication to USERS describing how  
1959 they collect, generate, use, transmit, and store personal information.

1960

1961 PRIVACY-7. USER DATA CONTROL

1962 Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete  
1963 personal information.

## 1964 PRIVACY-8. THIRD-PARTY LIMITATIONS

1965 Wherever USERS make choices regarding the treatment of their personal information, those  
1966 choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it  
1967 transmits the personal information.

1968  
1969 PRIVACY-9. USER NOTICE OF CHANGES

1970 Entities MUST, upon any material changes to a service or process that affects the prior or  
1971 ongoing collection, generation, use, transmission, or storage of USERS' personal information,  
1972 notify those USERS, and provide them with compensating controls designed to mitigate privacy  
1973 risks that may arise from those changes, which may include seeking express affirmative consent  
1974 of USERS in accordance with relevant law or regulation.

1975  
1976 PRIVACY-10. USER OPTION TO DECLINE

1977 USERS MUST have the opportunity to decline ~~registration~~Registration; decline credential  
1978 provisioning; decline the presentation of their credentials; and decline release of their  
1979 attributes or claims.

1980  
1981 PRIVACY-11. OPTIONAL INFORMATION

1982 Entities MUST clearly indicate to USERS what personal information is mandatory and what  
1983 information is optional prior to the transaction.

1984  
1985 PRIVACY-12. ANONYMITY

1986 Wherever feasible, entities MUST utilize identity systems and processes that enable  
1987 transactions that are anonymous, anonymous with validated attributes, pseudonymous, or  
1988 where appropriate, uniquely identified. Where applicable to such transactions, entities  
1989 employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES  
1990 collecting USER personal information. Organizations MUST request individuals' credentials only  
1991 when necessary for the transaction and then only as appropriate to the risk associated with the  
1992 transaction or only as appropriate to the risks to the ~~parties~~Participants associated with the  
1993 transaction.

1994  
1995 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

1996 Controls on the processing or use of USERS' personal information MUST be commensurate with  
1997 the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by  
1998 entities who conduct digital identity management functions, to establish what risks those  
1999 functions pose to USERS' privacy.

2000  
2001 PRIVACY-14. DATA RETENTION AND DISPOSAL

2002 Entities MUST limit the retention of personal information to the time necessary for providing  
2003 and administering the functions and services to USERS for which the information was collected,  
2004 except as otherwise required by law or regulation. When no longer needed, personal  
2005 information MUST be securely disposed of in a manner aligning with appropriate industry  
2006 standards and/or legal requirements.

2007

## 2008 PRIVACY-15. ATTRIBUTE SEGREGATION

2009 Wherever feasible, identifier data MUST be segregated from attribute data.

## 2010 SECURE-1. SECURITY PRACTICES

2011 Entities MUST apply appropriate and industry-accepted information security STANDARDS,  
2012 guidelines, and practices to the systems that support their identity functions and services.

2013

## 2014 SECURE-2. DATA INTEGRITY

2015 Entities MUST implement industry-accepted practices to protect the confidentiality and  
2016 integrity of identity data—including authentication data and attribute values—during the  
2017 execution of all digital identity management functions, and across the entire data lifecycle  
2018 (collection through destruction).

2019

## 2020 SECURE-3. CREDENTIAL REPRODUCTION

2021 Entities that issue or manage credentials and tokens MUST implement industry-accepted  
2022 processes to protect against their unauthorized disclosure and reproduction.

2023

## 2024 SECURE-4. CREDENTIAL PROTECTION

2025 Entities that issue or manage credentials and tokens MUST implement industry-accepted data  
2026 integrity practices to enable individuals and other entities to verify the source of credential and  
2027 token data.

2028

## 2029 SECURE-5. CREDENTIAL ISSUANCE

2030 Entities that issue or manage credentials and tokens MUST do so in a manner designed to  
2031 assure that they are granted to the appropriate and intended USER(s) only. Where  
2032 ~~registration~~[Registration](#) and credential issuance are executed by separate entities, procedures  
2033 for ensuring accurate exchange of ~~registration~~[Registration](#) and issuance information that are  
2034 commensurate with the stated assurance level MUST be included in business agreements and  
2035 operating policies.

2036

## 2037 SECURE-6. CREDENTIAL UNIQUENESS

2038 Entities that issue or manage credentials MUST ensure that each account to credential pairing is  
2039 uniquely identifiable within its namespace for authentication purposes.

2040

## 2041 SECURE-7. TOKEN CONTROL

2042 Entities that authenticate a USER MUST employ industry-accepted secure authentication  
2043 protocols to demonstrate the USER's control of a valid token.

2044

## 2045 SECURE-8. MULTIFACTOR AUTHENTICATION

2046 Entities that authenticate a USER MUST offer authentication mechanisms which augment or are  
2047 alternatives to a password.

2048

## 2049 SECURE-9. AUTHENTICATION RISK ASSESSMENT

2050 Entities MUST have a risk assessment process in place for the selection of authentication  
2051 mechanisms and supporting processes.

2052  
2053  
2054  
2055 SECURE-10. UPTIME  
2056 Entities that provide and conduct digital identity management functions MUST have established  
2057 policies and processes in place to maintain their stated assurances for availability of their  
2058 services.  
2059  
2060 SECURE-11. KEY MANAGEMENT  
2061 Entities that use cryptographic solutions as part of identity management MUST implement key  
2062 management policies and processes that are consistent with industry-accepted practices.  
2063  
2064 SECURE-12. RECOVERY AND REISSUANCE  
2065 Entities that issue credentials and tokens MUST implement methods for reissuance, updating,  
2066 and recovery of credentials and tokens that preserve the security and assurance of the original  
2067 ~~registration~~[Registration](#) and credentialing operations.  
2068  
2069 SECURE-13. REVOCATION  
2070 Entities that issue credentials or tokens MUST have processes and procedures in place to  
2071 invalidate credentials and tokens.  
2072  
2073 SECURE-14. SECURITY LOGS  
2074 Entities conducting digital identity management functions MUST log their transactions and  
2075 security events, in a manner that supports system audits and, where necessary, security  
2076 investigations and regulatory requirements. Timestamp synchronization and detail of logs  
2077 MUST be appropriate to the level of risk associated with the environment and transactions.  
2078  
2079 SECURE-15. SECURITY AUDITS  
2080 Entities MUST conduct regular audits of their compliance with their own information security  
2081 policies and procedures, and any additional requirements of law, including a review of their  
2082 logs, incident reports and credential loss occurrences, and MUST periodically review the  
2083 effectiveness of their policies and procedures in light of that data.  
2084

DRAFT

2086

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

2088