

COMMONWEALTH OF VIRGINIA



IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT Federation and Participant Requirements

Table of Contents

1 Publication Version Control 1
2 Reviews 1
3 Purpose and Scope 1
4 Statutory Authority 2
5 Definitions 3
6 Background 15
7 Minimum Specifications 16

DRAFT

1 Publication Version Control

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

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

2 Reviews

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

3 Purpose and Scope

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

29 4 Statutory Authority

30

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

35

36 **Governing Statutes:**

37

38 **Secretary of Technology**

39 § 2.2-225. Position established; agencies for which responsible; additional powers

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

41

42 **Identity Management Standards Advisory Council**

43 § 2.2-437. Identity Management Standards Advisory Council

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

45

46 **Commonwealth Identity Management Standards**

47 § 2.2-436. Approval of electronic identity standards

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

49

50 **Electronic Identity Management Act**

51 Chapter 50. Electronic Identity Management Act

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

53

54

55

56

57

58

59

60 5 Definitions

61
62 Terms used in this document comply with definitions in the Public Review version of the
63 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3),
64 and align with adopted definitions in § 59.1-550, *Code of Virginia* (COV), and the
65 Commonwealth of Virginia's ITRM Glossary (ITRM Glossary).¹

66
67 Active Attack: An online attack where the attacker transmits data to the claimant, credential
68 service provider, verifier, or relying Participant. Examples of active attacks include man-in-the-
69 middle, impersonation, and session hijacking.

70
71 Address of Record: The official location where an individual can be found. The address of record
72 always includes the residential street address of an individual and may also include the mailing
73 address of the individual. In very limited circumstances, an Army Post Office box number, Fleet
74 Post Office box number or the street address of next of kin or of another contact individual can
75 be used when a residential street address for the individual is not available.

76
77 Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An
78 algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2)
79 adopted in a FIPS or NIST Recommendation.

80
81 Applicable Law: Laws, statutes, regulations, and rules of the jurisdiction in which the members
82 of an Identity Trust Framework operates.

83
84 Applicant: A Participant undergoing the processes of Registration and Identity Proofing.

85
86 Assertion: A statement from a verifier to a relying Participant (RP) that contains identity
87 information about a Subscriber. Assertions may also contain verified attributes.

88
89 Assertion Reference: A data object, created in conjunction with an Assertion, which identifies
90 the verifier and includes a pointer to the full Assertion held by the verifier.

91
92 Assurance: In the context of [OMB M-04-04]² and this document, assurance is defined as 1) the
93 degree of confidence in the vetting process used to establish the identity of an individual to
94 whom the credential was issued, and 2) the degree of confidence that the individual who uses
95 the credential is the individual to whom the credential was issued.

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

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

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

- 96 Assurance Model: Policies, processes, and protocols that define how Assurance will be
97 established in an Identity Trust Framework.
98
- 99 Asymmetric Keys: Two related keys, a public key and a private key that are used to perform
100 complementary operations, such as encryption and decryption or signature generation and
101 signature verification.
102
- 103 Attack: An attempt by an unauthorized individual to fool a verifier or a relying Participant into
104 believing that the unauthorized individual in question is the Subscriber.
105
- 106 Attacker: A Participant who acts with malicious intent to compromise an Information System.
107
- 108 Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or
109 something.
110
- 111 Authentication: The process of establishing confidence in the identity of users or Information
112 Systems.
113
- 114 Authentication Protocol: A defined sequence of messages between a claimant and a verifier
115 that demonstrates that the claimant has possession and control of a valid authenticator to
116 establish his/her identity, and optionally, demonstrates to the claimant that he or she is
117 communicating with the intended verifier.
118
- 119 Authentication Protocol Run: An exchange of messages between a claimant and a verifier that
120 results in authentication (or authentication failure) between the two Participants.
121
- 122 Authentication Secret: A generic term for any secret value that could be used by an attacker to
123 impersonate the Subscriber in an authentication protocol. These are further divided into short-
124 term authentication secrets, which are only useful to an attacker for a limited period of time,
125 and long-term authentication secrets, which allow an attacker to impersonate the Subscriber
126 until they are manually reset. The authenticator secret is the canonical example of a long term
127 authentication secret, while the authenticator output, if it is different from the authenticator
128 secret, is usually a short term authentication secret.
129
- 130 Authenticator: Something that the claimant possesses and controls (typically a cryptographic
131 module or password) that is used to authenticate the claimant's identity. In previous versions of
132 this guideline, this was referred to as a token.
133
- 134 Authenticator Assurance Level (AAL): A metric describing robustness of the authentication
135 process proving that the claimant is in control of a given Subscriber's authenticator(s).
136
- 137 Authenticator Output: The output value generated by an authenticator. The ability to generate
138 valid authenticator outputs on demand proves that the claimant possesses and controls the

139 authenticator. Protocol messages sent to the verifier are dependent upon the authenticator
140 output, but they may or may not explicitly contain it.

141

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

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

144

145 Bearer Assertion: An Assertion that does not provide a mechanism for the Subscriber to prove
146 that he or she is the rightful owner of the Assertion. The RP has to assume that the Assertion
147 was issued to the Subscriber who presents the Assertion or the corresponding Assertion
148 reference to the RP.

149

150 Bit: A binary digit: 0 or 1.

151

152 Biometrics: Automated recognition of individuals based on their behavioral and biological
153 characteristics. In this document, biometrics may be used to unlock authenticators and prevent
154 repudiation of Registration.

155

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

157

158 Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally
159 signed by a Certificate Authority. [RFC 5280]³

160

161 Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant
162 a challenge (usually a random value or a nonce) that the claimant combines with a secret (such
163 as by hashing the challenge and a shared secret together, or by applying a private key operation
164 to the challenge) to generate a response that is sent to the verifier. The verifier can
165 independently verify the response generated by the claimant (such as by re-computing the hash
166 of the challenge and the shared secret and comparing to the response, or performing a public
167 key operation on the response) and establish that the claimant possesses and controls the
168 secret.

169

170 Claimant: A Participant whose identity is to be verified using an authentication protocol.

171 Claimed Address: The physical location asserted by an individual (e.g. an applicant) where
172 he/she can be reached. It includes the residential street address of an individual and may also
173 include the mailing address of the individual. For example, a person with a foreign passport,
174 living in the U.S., will need to give an address when going through the Identity Proofing process.
175 This address would not be an "address of record" but a "claimed address."

176

177 Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth
178 and address. [GPG45]⁴

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

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

183

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

186

187 Credential: An object or data structure that authoritatively binds an identity (and optionally,
188 additional attributes) to an authenticator possessed and controlled by a Subscriber. While
189 common usage often assumes that the credential is maintained by the Subscriber, this
190 document also uses the term to refer to electronic records maintained by the CSP which
191 establish a binding between the Subscriber's authenticator(s) and identity.

192

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

197

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

204

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

210

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

215

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

217

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

218 Data Integrity: The property that data has not been altered by an unauthorized entity.
219

220 Derived Credential: A credential issued based on proof of possession and control of an
221 authenticator associated with a previously issued credential, so as not to duplicate the Identity
222 Proofing process.
223

224 Digital Identity System: An Information System that supports Electronic Authentication and the
225 management of a person's Identity in a digital environment. [Referenced in § 59.1-550, COV]
226

227 Digital Signature: An asymmetric key operation where the private key is used to digitally sign
228 data and the public key is used to verify the signature. Digital signatures provide authenticity
229 protection, integrity protection, and non-repudiation.
230

231 Eavesdropping Attack: An attack in which an attacker listens passively to the authentication
232 protocol to capture information which can be used in a subsequent active attack to
233 masquerade as the claimant.
234

235 Electronic Authentication: The process of establishing confidence in user identities
236 electronically presented to an Information System.
237

238 Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value
239 of a secret. Entropy is usually stated in bits.
240

241 Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes
242 a class of data objects called XML documents and partially describes the behavior of computer
243 programs which process them.
244

245 Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal
246 Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI
247 Policy Authority to create, sign, and issue public key certificates to Principal CAs.
248

249 Federal Information Security Management Act (FISMA): Title III of the E-Government Act
250 requiring each federal agency to develop, document, and implement an agency-wide program
251 to provide information security for the information and Information Systems that support the
252 operations and assets of the agency, including those provided or managed by another agency,
253 contractor, or other source.
254

255 Federal Information Processing Standard (FIPS): Under the Information Technology
256 Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards
257 and guidelines that are developed by the National Institute of Standards and Technology (NIST)
258 for Federal computer systems. These standards and guidelines are issued by NIST as Federal
259 Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when

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

262

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

266

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

269

270 Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string.

271 Approved hash functions satisfy the following properties:

272

- (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and

273

- (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

274

275

276

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

281

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

283

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

286

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

289

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

293

294 Identity Trust Framework: A Digital Identity System with established identity, security, privacy,
295 technology, and enforcement rules and policies adhered to by certified identity providers that
296 are members of the Identity Trust Framework. Members of an Identity Trust Framework
297 include Identity Trust Framework operators and identity providers. Relying Participants may be,
298 but are not required to be, a member of an Identity Trust Framework in order to accept an
299 identity credential issued by a certified identity provider to verify an identity credential holder's
300 identity. [§ 59.1-550, COV]

301

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

302 Information System: A discrete set of information resources organized for the collection,
303 processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST
304 Interagency/Internal Report (IR) 7298 r. 2]
305

306 Kerberos: A widely used authentication protocol developed at MIT. In “classic” Kerberos, users
307 share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to
308 communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by
309 the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords,
310 the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who
311 capture the initial user-to- KDC exchange. Longer password length and complexity provide
312 some mitigation to this vulnerability, although sufficiently long passwords tend to be
313 cumbersome for users.
314

315 Knowledge Based Authentication: Authentication of an individual based on knowledge of
316 information associated with his or her claimed identity in public databases. Knowledge of such
317 information is considered to be private rather than secret, because it may be used in contexts
318 other than authentication to a verifier, thereby reducing the overall assurance associated with
319 the authentication process.
320

321 Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the
322 attacker positions himself or herself in between the claimant and verifier so that he can
323 intercept and alter data traveling between them.
324

325 Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric
326 key to detect both accidental and intentional modifications of the data. MACs provide
327 authenticity and integrity protection, but not non-repudiation protection.
328

329 Multi-Factor: A characteristic of an authentication system or an authenticator that uses more
330 than one authentication factor. The three types of authentication factors are something you
331 know, something you have, and something you are.
332

333 Network: An open communications medium, typically the Internet, that is used to transport
334 messages between the claimant and other Participants. Unless otherwise stated, no
335 assumptions are made about the security of the network; it is assumed to be open and subject
336 to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e.,
337 eavesdropping) attack at any point between the Participants (e.g., claimant, verifier, CSP or RP).
338

339 Nonce: A value used in security protocols that is never repeated with the same key. For
340 example, nonces used as challenges in challenge-response authentication protocols must not
341 be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay
342 attack. Using a nonce as a challenge is a different requirement than a random challenge,
343 because a nonce is not necessarily unpredictable.
344

345 Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on
346 an authentication protocol run or by penetrating a system and stealing security files) that
347 he/she is able to analyze in a system of his/her own choosing.
348

349 Online Attack: An attack against an authentication protocol where the attacker either assumes
350 the role of a claimant with a genuine verifier or actively alters the authentication channel.
351

352 Online Guessing Attack: An attack in which an attacker performs repeated logon trials by
353 guessing possible values of the authenticator output.
354

355 Operational Authority: Entity responsible for operations, maintenance, management, and
356 related functions of an Identity Trust Framework.
357

358 Participant Requirements: A set of rules and policies in an Identity Trust Framework addressing
359 identity, security, privacy, technology, and enforcement, which are assigned to each member
360 type in a Digital Identity System. Member types include Registration Authorities (RAs), Identity
361 Providers (IdPs), Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs).
362 [§ 59.1-550, COV]
363

364 Passive Attack: An attack against an authentication protocol where the attacker intercepts data
365 traveling along the network between the claimant and verifier, but does not alter the data (i.e.,
366 eavesdropping).
367

368 Password: A secret that a claimant memorizes and uses to authenticate his or her identity.
369 Passwords are typically character strings.
370

371 Personal Identification Number (PIN): A password consisting only of decimal digits.
372

373 Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g.,
374 identity card, smart card) issued to federal employees and contractors that contains stored
375 credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that
376 the claimed identity of the cardholder can be verified against the stored credentials by another
377 person (human readable and verifiable) or an automated process (computer readable and
378 verifiable).
379

380 Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally
381 Identifiable Information means information that can be used to distinguish or trace an
382 individual's identity, either alone or when combined with other information that is linked or
383 linkable to a specific individual.
384

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

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

392

393 Physical In-Person: Method of Identity Proofing in which Applicants are required to physically
394 present themselves and identity evidence to a representative of the Registration Authority or
395 Identity Trust Framework. [NIST SP 800-63-2]

396

397 Possession and control of an authenticator: The ability to activate and use the authenticator in
398 an authentication protocol.

399

400 Practice Statement: A formal statement of the practices followed by the Participants to an
401 authentication process (i.e., RA, CSP, or verifier). It usually describes the policies and practices
402 of the Participants and can become legally binding.

403

404 Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can
405 be used to compromise the authenticator.

406

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

409

410 Protected Session: A session wherein messages between two participants are encrypted and
411 integrity is protected using a set of shared secrets called session keys. A participant is said to be
412 authenticated if, during the session, he, she or it proves possession of a long term authenticator
413 in addition to the session keys, and if the other Participant can verify the identity associated
414 with that authenticator. If both participants are authenticated, the protected session is said to
415 be mutually authenticated.

416

417 Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to
418 infer the Subscriber but which does permit the RP to associate multiple interactions with the
419 Subscriber's claimed identity.

420

421 Public Credentials: Credentials that describe the binding in a way that does not compromise the
422 authenticator.

423

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

426

427 Public Key Certificate: A digital document issued and digitally signed by the private key of a
428 Certificate authority that binds the name of a Subscriber to a public key. The certificate
429 indicates that the Subscriber identified in the certificate has sole control and access to the
430 private key. See also [RFC 5280].

431

432 Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and
433 workstations used for the purpose of administering certificates and public-private key pairs,
434 including the ability to issue, maintain, and revoke public key certificates.
435

436 Registration: The process through which an applicant applies to become a Subscriber of a CSP
437 and an RA validates the identity of the applicant on behalf of the CSP.
438

439 Registration Authority (RA): A trusted entity that establishes and vouches for the identity or
440 attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be
441 independent of a CSP, but it has a relationship to the CSP(s).
442

443 Relying Party (RP): An entity that relies upon the Subscriber's authenticator(s) and credentials
444 or a verifier's Assertion of a claimant's identity, typically to process a transaction or grant access
445 to information or a system.
446

447 Remote: (As in remote authentication or remote transaction) An information exchange
448 between network-connected devices where the information cannot be reliably protected end-
449 to-end by a single organization's security controls. Note: Any information exchange across the
450 Internet is considered remote.
451

452 Replay Attack: An attack in which the attacker is able to replay previously captured messages
453 (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or
454 vice versa.
455

456 Risk Assessment: The process of identifying the risks to system security and determining the
457 probability of occurrence, the resulting impact, and additional safeguards that would mitigate
458 this impact. Part of Risk Management and synonymous with Risk Analysis.
459

460 Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the
461 results of computations for one instance cannot be reused by an attacker.
462

463 Secondary Authenticator: A temporary secret, issued by the verifier to a successfully
464 authenticated Subscriber as part of an Assertion protocol. This secret is subsequently used, by
465 the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer
466 Assertions, Assertion references, and Kerberos session keys.
467

468 Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in
469 browsers and web servers. SSL has been superseded by the newer Transport Layer Security
470 (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.
471

472 Security Assertion Mark-up Language (SAML): An XML-based security specification developed
473 by the Organization for the Advancement of Structured Information Standards (OASIS) for
474 exchanging authentication (and authorization) information between trusted entities over the
475 Internet.

476 SAML Authentication Assertion: A SAML Assertion that conveys information from a verifier to
477 an RP about a successful act of authentication that took place between the verifier and a
478 Subscriber.
479

480 Session Hijack Attack: An attack in which the attacker is able to insert himself or herself
481 between a claimant and a verifier subsequent to a successful authentication exchange between
482 the latter two Participants. The attacker is able to pose as a Subscriber to the verifier or vice
483 versa to control session data exchange. Sessions between the claimant and the relying
484 Participant can also be similarly compromised.
485

486 Shared Secret: A secret used in authentication that is known to the claimant and the verifier.
487

488 Social Engineering: The act of deceiving an individual into revealing sensitive information by
489 associating with the individual to gain confidence and trust.
490

491 Special Publication (SP): A type of publication issued by NIST. Specifically, the Special
492 Publication 800-series reports on the Information Technology Laboratory's research, guidelines,
493 and outreach efforts in computer security, and its collaborative activities with industry,
494 government, and academic organizations.
495

496 Strongly Bound Credentials: Credentials that describe the binding between a user and
497 authenticator in a tamper-evident fashion.
498

499 Subscriber: A Participant who has received a credential or authenticator from a CSP.
500

501 Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation
502 and its inverse, for example to encrypt and decrypt, or create a message authentication code
503 and to verify the code.
504

505 Token: See Authenticator.
506

507 Token Authenticator: See Authenticator Output.
508

509 Token Secret: See Authenticator Secret.
510

511 Transport Layer Security (TLS): An authentication and security protocol widely implemented in
512 browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure
513 Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52,
514 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies
515 how TLS is to be used in government applications.
516

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

520 Unverified Name: A Subscriber name that is not verified as meaningful by Identity Proofing.
521
522 Valid: In reference to an ID, the quality of not being expired or revoked.
523
524 Verified Name: A Subscriber name that has been verified by Identity Proofing.
525
526 Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and
527 control of one or two authenticators using an authentication protocol. To do this, the verifier
528 may also need to validate credentials that link the authenticator(s) and identity and check their
529 status.
530
531 Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an
532 authentication protocol, usually to capture information that can be used to masquerade as a
533 claimant to the real verifier.
534
535 Virtual In-Person Proofing: A remote identity person proofing process that employs technical
536 and procedural measures that provide sufficient confidence that the remote session can be
537 considered equivalent to a physical, in-person identity proofing encounter. [NIST SP 800-63A]
538
539 Weakly Bound Credentials: Credentials that describe the binding between a user and
540 authenticator in a manner than can be modified without invalidating the credential.
541
542 Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero
543 so that the data is destroyed and not recoverable. This is often contrasted with deletion
544 methods that merely destroy reference to data within a file system rather than the data itself.
545
546 Zero-knowledge Password Protocol: A password based authentication protocol that allows a
547 claimant to authenticate to a Verifier without revealing the password to the verifier. Examples
548 of such protocols are EKE, SPEKE and SRP.

549 6 Background

550

551 In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter
552 50 of Title 59.1, *Code of Virginia*) to address demand in the state’s digital economy for secure,
553 privacy enhancing Electronic Authentication and identity management. Growing numbers of
554 “communities of interest” have advocated for stronger, scalable and interoperable identity
555 solutions to increase consumer protection and reduce liability for principal actors in the identity
556 ecosystem – Identity Providers, Credential Service Providers and Relying Parties.

557

558 To address the demand contemplated by the Electronic Identity Management Act, the General
559 Assembly also created the Identity Management Standards Advisory Council (IMSAC) to advise
560 the Secretary of Technology on the adoption of identity management standards and the
561 creation of guidance documents, pursuant to §2.2-436. A copy of the IMSAC Charter has been
562 provided in **Appendix 1**.

563

564 The Advisory Council recommends to the Secretary of Technology guidance documents relating
565 to (i) nationally recognized technical and data standards regarding the verification and
566 authentication of identity in digital and online transactions; (ii) the minimum specifications and
567 standards that should be included in an Identity Trust Framework, as defined in §59.1-550, so
568 as to warrant liability protection pursuant to the Electronic Identity Management Act (§59.1-
569 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by
570 third Participants on identity credentials, as defined in §59.1-550.

571

572 Purpose Statement

573

574 This guidance document, as defined in § 2.2-4001, was developed by the Identity Management
575 Standards Advisory Council (IMSAC), on behalf of the Secretary of Technology, to provide
576 information or guidance of general applicability to the public for interpreting or implementing
577 the Electronic Identity Management Act. Specifically, the document establishes minimum
578 specifications for Federation and Participant Requirements in a Digital Identity System. The
579 minimum specifications have been designed to be conformant with NIST SP 800-63C.

580

581 The document defines governance models, processes, assurance levels, and Participant
582 Requirements for a Federated Digital Identity System. The document assumes that specific
583 Participant Requirements will be established in the Identity Trust Framework for each distinct
584 Digital Identity System, and that these requirements will be designed based on the Electronic
585 Authentication model and Federation Assurance Level (FAL) requirements for the system.

586

587 The document limits its focus to Federation and Participant Requirements. Minimum
588 specifications for other components of a Digital Identity System have been defined in separate
589 IMSAC guidance documents in this series, pursuant to §2.2-436 and §2.2-437.

590

591 7 Minimum Specifications

592
593 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3)
594 defines an “Federation” in a Digital Identity System as “A process that allows for the
595 conveyance of identity and authentication information across a set of networked systems.”¹²
596 Federation of a Digital Identity System depends upon each member, or Participant, in the
597 system complying with Participant Requirements, the set of rules and policies assigned to each
598 member type by the system’s Identity Trust Framework.

599
600 This document establishes minimum specifications for Federation and Participant
601 Requirements in a Digital Identity System conformant with NIST SP 800-63-3. However, the
602 minimum specifications defined in this document have been developed to accommodate
603 requirements for Federation and Participant Requirements established under other national
604 and international standards.¹³ Minimum specifications for other components of a Digital
605 Identity System have been documented in separate guidance documents in the IMSAC series,
606 pursuant to §2.2-436 and §2.2-437.

607 608 Electronic Authentication Model

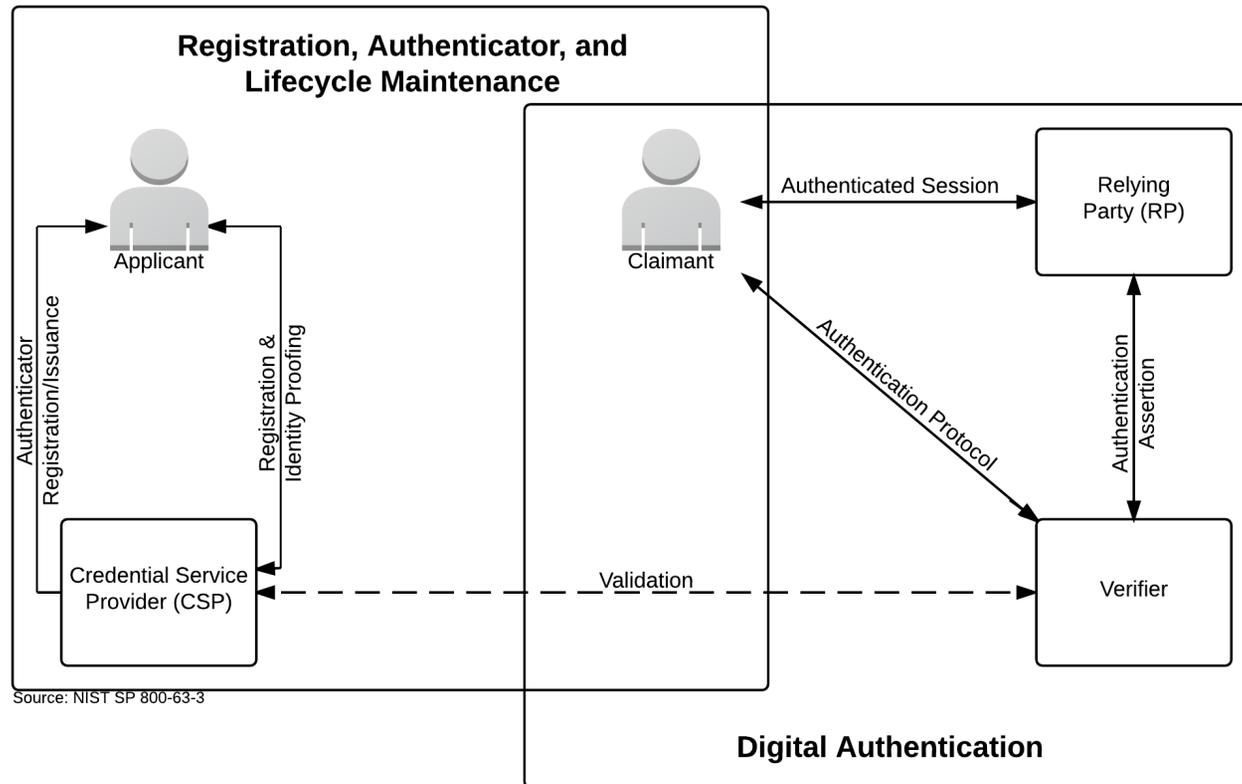
609
610 Electronic Authentication is the process of establishing confidence in individual identities
611 presented to a Digital Identity System. In a Federated Digital Identity Systems, Electronic
612 Authentication and related flows of identity information occur across a set of network systems.
613 These systems are often run and controlled by disparate members in different network and
614 security domains. Therefore, Federation requires Electronic Authentication models to be
615 extended to take into account the roles played by each member type and the corresponding
616 Participant Requirements.

617
618 The minimum specifications for Federation and Participant Requirements defined in this
619 document reflect the Electronic Authentication model used primarily by governmental entities.
620 More complex models that separate functions among a broader range of Participants are also
621 available and may have advantages in some classes of applications. While a simpler model
622 serves as the basis for these minimum specifications, it does not preclude members in Digital
623 Identity Systems from separating these functions. Minimum specifications for the Electronic
624 Authentication model reflected in this document have been defined in *IMSAC Guidance*
625 *Document: Electronic Authentication*, and a graphic of the model has been shown in **Figure 1**.

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

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

626 **Figure 1. Electronic Authentication Model**



627
 628
 629
 630
 631
 632
 633

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.

634 Federation

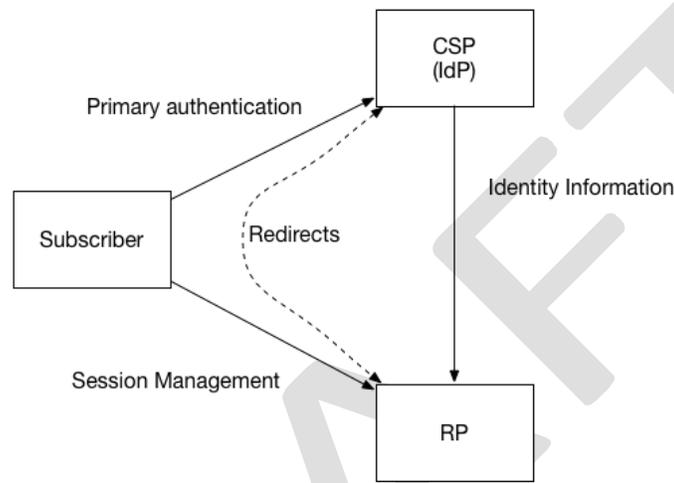
635

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

640

641 **Figure 2: Federation Model**

642



643

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

651

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

658

659 The RP communication with the IdP reveals to the IdP where the Subscriber is conducting a
660 transaction. Communications from multiple RPs allow the IdP to build a profile of Subscriber
661 transactions that would not have existed absent Federation. This aggregation could enable new
662 capabilities for Subscriber tracking and use of profile information that do not align with the
663 privacy interests of the Subscribers.

664

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

671

672 Federation Models

673

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

678

679 Central Authority

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

684

685 Most Federations using the central authority model have a simple membership model - either
686 Participants are in the Federation or they are not. However, more sophisticated Federations
687 have multiple tiers of membership which can be used by Federated Participants to tell whether
688 other Participants in the Federation have been more thoroughly vetted or have some common
689 purpose that justifies a higher level of access. As a consequence, some Participants in the
690 Federation are more likely to automatically release information about their Subscribers to the
691 Participants in the higher tiers.

692

693 Manual Registration

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

699

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

702

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

706

707

708

709 Dynamic Registration

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

715

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

722

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

732

733 Proxied Federation

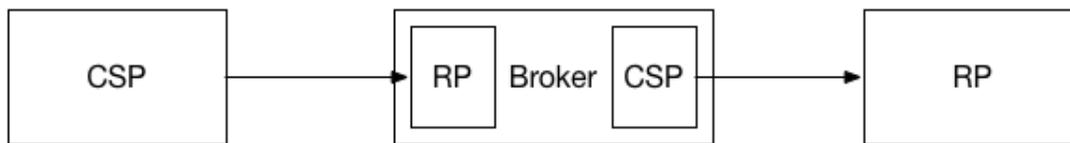
734 In a proxied Federation model, the communication between the IdP and the RP is proxied in a
735 way that prevents direct communication between the two Participants. There may be multiple
736 methods of achieving this effect, but common configurations include a third Participant that
737 acts as a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

739

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

744

745

746 **Figure 3: Federation Proxy Model**747
748

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

756

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

766

767 The following list documents a spectrum of blinding implementations:

768

- 769 • The Federation proxy does not blind the RP and IdP from one another. The Federation
770 proxy is able to monitor and track all Subscriber relationships between the RPs and IdPs,
771 and has visibility into any attributes it is transmitting in the Assertions.

771

- 772 • The Federation proxy does not blind the RP and IdP from one another. The Federation
773 proxy is able to monitor and track all Subscriber relationships between the RPs and IdPs,
774 but has no visibility into any attributes it is transmitting in the Assertions.

774

- 775 • The Federation proxy blinds the RP and IdP from each other. The Federation proxy is
776 able to monitor and track all Subscriber relationships between the RPs and IdPs, and has
777 visibility into any attributes it is transmitting in the Assertions.

777

- 778 • The Federation proxy blinds the RP and IdP from each other. The Federation proxy is
779 able to monitor and track all Subscriber relationships between the RPs and IdPs, but has
780 no visibility into any attributes it is transmitting in the Assertions.

780

- 781 • The Federation proxy blinds the RP, IdP, and itself. The Federation proxy cannot monitor
782 or track any Subscriber relationships, and has no visibility into any attributes it is
783 transmitting in the Assertions.

783

784 Runtime Decisions

785

786 The fact that Federated Participants are known to each other through some form of registration
787 or centralized management does not necessarily mean they are allowed to pass information.

788 Federated Participants can establish whitelists of other Federated Participants who may
789 authenticate Subscribers or pass information about them without runtime authorization from
790 the Subscriber.

791

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

796

797 Federation Assurance Level

798

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

802

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

808

809 Examples of Assertions Protocols:

810

- 811 • SAML Assertions – Security Assertion Markup Language (SAML) Assertions are specified
812 using a mark-up language intended for describing security Assertions. They can be used
813 by a verifier to make a statement to an RP about the identity of a claimant. SAML
assertions may optionally be digitally signed.

814

- 815 • OpenID Connect Claims - OpenID Connect are specified using JavaScript Object Notation
816 (JSON) for describing security, and optionally, user claims. JSON user info claims may
optionally be digitally signed.

817

- 818 • Kerberos Tickets – Kerberos Tickets allow a ticket granting authority to issue session
819 keys to two authenticated parties using based encapsulation schemes.

819

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

824

825

826

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

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

828

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

832

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

838

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

844

845 **Participant Requirements**

846

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

852

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

858

859 Registration Authorities (RAs)

860 RAs establish and vouch for the Identity or Attributes of an Applicant to a CSP. RAs may be an
861 integral part of a CSP, or it may be independent of a CSP, but it maintains a trusted relationship
862 to the CSP(s). Primary requirements for RAs include the following:

- 863 • Perform Physical or Virtual In-Person Proofing functions on identity evidence submitted
864 by an Applicant for a Claimed Identity
- 865 • Verify and validate identity evidence submitted by an Applicant to support a Claimed
866 Identity during a Registration event.
- 867 • Perform Registration (or enrollment) of Applicants for which the Claimed Identity has
868 been verified, validated, and accepted
- 869 • Issue an appropriate Credential to a registered Subscriber who has completed the
870 Registration process
- 871 • Manage, monitor, and audit the usage of Credentials by Subscribers who have
872 Registered with the RA
- 873 • Establish and implement a process to revoke a Subscriber's Credential in the event of
874 improper use, irregularities, or a security breach
- 875 • Manage required post-issuance updates or modifications to a Subscriber's Credential
876 based on verified and validated changes in the Claimed Identity or identity evidence
- 877 • Establish and implement a process to re-issue a Subscriber's Credential when corrective
878 action has been taken or the identity evidence has been updated

879

880 Identity Providers (IdPs)

881 IdPs manage the Subscriber's primary authentication Credentials and issue Assertions derived
882 from those Credentials, generally to the CSP. Primary requirements for IdPs include the
883 following:

- 884 • Provide a trust model that ensures that an individual is linked to identities which have
885 been issued, protected, and managed to provide the accuracy of asserted Attributes
- 886 • Develop and provide an Authentication process by which the user (Subscriber or
887 Applicant) provides evidence to the IdP, who independently verifies that the user is who
888 he or she claims to be
- 889 • Develop a process to periodically reevaluate the status of the user and the validity of his
890 or her associated Identity
- 891 • Develop a process for Attribute management to ensure the timely cancellation or
892 modification of Attributes should the user's status change
- 893 • Develop a process for auditing the Attribute identification process, including registration
894 activities, to ensure Attributes are maintained in accordance with the process specified
895 by that IdP
- 896 • Conduct audit functions in a manner to identify any irregularities or security breaches
- 897 • Provide to the Federation audit information, upon request
- 898 • Provide a process to assist users who have either lost or forgotten their means of
899 Authentication

900

901

902 Credential Service Providers (CSPs)

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

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

912

913 Verifiers

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

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

922

923 Relying Parties

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

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

931

932

933

935 Privacy and Security

936

937 The minimum specifications established in this document for privacy and security in the use of
938 person information for Electronic Authentication apply the Fair Information Practice Principles
939 (FIPPs).¹⁶ The FIPPs have been endorsed by the National Strategy for Trusted Identities in
940 Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.¹⁷

941

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

945

946 The minimum specifications for Assertions apply the following FIPPs:

- 947 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants
948 regarding collection, use, dissemination, and maintenance of person information required
949 during the Registration, Identity Proofing and verification processes.
- 950 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using
951 person information and, to the extent practicable, seek consent for the collection, use,
952 dissemination, and maintenance of that information. RAs and CSPs also should provide
953 mechanisms for appropriate access, correction, and redress of person information.
- 954 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits
955 the collection of person information and specifically articulate the purpose or purposes for
956 which the information is intended to be used.
- 957 • Data Minimization: RAs and CSPs should collect only the person information directly
958 relevant and necessary to accomplish the Registration and related processes, and only
959 retain that information for as long as necessary to fulfill the specified purpose.
- 960 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for
961 the purpose specified in the notice. Disclosure or sharing that information should be limited
962 to the specific purpose for which the information was collected.
- 963 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that
964 person information is accurate, relevant, timely, and complete.
- 965 • Security: RAs and CSPs should protect personal information through appropriate security
966 safeguards against risks such as loss, unauthorized access or use, destruction, modification,
967 or unintended or inappropriate disclosure.
- 968 • Accountability and Auditing: RAs and CSPs should be accountable for complying with these
969 principles, providing training to all employees and contractors who use person information,
970 and auditing the actual use of person information to demonstrate compliance with these
971 principles and all applicable privacy protection requirements.

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

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

972 Appendix 1. IMSAC Charter

973

974

COMMONWEALTH OF VIRGINIA

975

IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL

976

CHARTER

977

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

979

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

983

984 The Advisory Council recommends to the Secretary of Technology guidance documents relating
985 to (i) nationally recognized technical and data standards regarding the verification and
986 authentication of identity in digital and online transactions; (ii) the minimum specifications and
987 standards that should be included in an Identity Trust Framework, as defined in § 59.1-550, so
988 as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-
989 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by
990 third Participants on identity credentials, as defined in § 59.1-550.

991

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

993

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

- 995 1. The Advisory Council consists of seven members, to be appointed by the Governor, with
996 expertise in electronic identity management and information technology. Members include
997 a representative of the Department of Motor Vehicles, a representative of the Virginia
998 Information Technologies Agency, and five representatives of the business community with
999 appropriate experience and expertise. In addition to the seven appointed members, the
1000 Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex
1001 officio member of the Advisory Council.
- 1002
- 1003 2. The Advisory Council designates one of its members as chairman.
- 1004
- 1005 3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure
1006 of the Governor, and may be reappointed.
- 1007
- 1008 4. Members serve without compensation but may be reimbursed for all reasonable and
1009 necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.
- 1010
- 1011 5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.
- 1012
- 1013

1014 The formation, membership and governance structure for the Advisory Council has been
1015 codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

1016

1017 The statutory authority and requirements for public notice and comment periods for guidance
1018 documents have been established pursuant to § 2.2-437.C, as follows:

1019

1020 C. Proposed guidance documents and general opportunity for oral or written submittals as to
1021 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published
1022 in the Virginia Register of Regulations as a general notice following the processes and
1023 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§
1024 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written
1025 comments following the posting and publication and shall hold at least one meeting dedicated
1026 to the receipt of oral comment no less than 15 days after the posting and publication. The
1027 Advisory Council shall also develop methods for the identification and notification of interested
1028 Participants and specific means of seeking input from interested persons and groups. The
1029 Advisory Council shall send a copy of such notices, comments, and other background material
1030 relative to the development of the recommended guidance documents to the Joint Commission
1031 on Administrative Rules.

1032

1033

1034 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the
1035 minutes of the meeting and related IMSAC documents, visit:
1036 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

1037 Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline
1038 Functional Requirements (v.1.0) for Privacy and Security

1039

1040 PRIVACY-1. DATA MINIMIZATION

1041 Entities MUST limit the collection, use, transmission and storage of personal information to the
1042 minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities
1043 providing claims or attributes MUST NOT provide any more personal information than what is
1044 requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to
1045 accommodate information requests of variable granularity, to support data minimization.

1046

1047 PRIVACY-2. PURPOSE LIMITATION

1048 Entities MUST limit the use of personal information that is collected, used, transmitted, or
1049 stored to the specified purposes of that transaction. Persistent records of contracts, assurances,
1050 consent, or legal authority MUST be established by entities collecting, generating, using,
1051 transmitting, or storing personal information, so that the information, consistently is used in
1052 the same manner originally specified and permitted.

1053

1054 PRIVACY-3. ATTRIBUTE MINIMIZATION

1055 Entities requesting attributes MUST evaluate the need to collect specific attributes in a
1056 transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST
1057 collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever
1058 feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities
1059 MUST be bound to claims instead of actual attribute values.

1060

1061 PRIVACY-4. CREDENTIAL LIMITATION

1062 Entities MUST NOT request USERS' credentials unless necessary for the transaction and then
1063 only as appropriate to the risk associated with the transaction or to the risks to the Participants
1064 associated with the transaction.

1065

1066 PRIVACY-5. DATA AGGREGATION RISK

1067 Entities MUST assess the privacy risk of aggregating personal information, in systems and
1068 processes where it is collected, generated, used, transmitted, or stored, and wherever feasible,
1069 MUST design and operate their systems and processes to minimize that risk. Entities MUST
1070 assess and limit linkages of personal information across multiple transactions without the
1071 USER's explicit consent.

1072

1073 PRIVACY-6. USAGE NOTICE

1074 Entities MUST provide concise, meaningful, and timely communication to USERS describing how
1075 they collect, generate, use, transmit, and store personal information.

1076

1077 PRIVACY-7. USER DATA CONTROL

1078 Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete
1079 personal information.

1080 PRIVACY-8. THIRD-PARTY LIMITATIONS

1081 Wherever USERS make choices regarding the treatment of their personal information, those
1082 choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it
1083 transmits the personal information.

1084

1085 PRIVACY-9. USER NOTICE OF CHANGES

1086 Entities MUST, upon any material changes to a service or process that affects the prior or
1087 ongoing collection, generation, use, transmission, or storage of USERS' personal information,
1088 notify those USERS, and provide them with compensating controls designed to mitigate privacy
1089 risks that may arise from those changes, which may include seeking express affirmative consent
1090 of USERS in accordance with relevant law or regulation.

1091

1092 PRIVACY-10. USER OPTION TO DECLINE

1093 USERS MUST have the opportunity to decline Registration; decline credential provisioning;
1094 decline the presentation of their credentials; and decline release of their attributes or claims.

1095

1096 PRIVACY-11. OPTIONAL INFORMATION

1097 Entities MUST clearly indicate to USERS what personal information is mandatory and what
1098 information is optional prior to the transaction.

1099

1100 PRIVACY-12. ANONYMITY

1101 Wherever feasible, entities MUST utilize identity systems and processes that enable
1102 transactions that are anonymous, anonymous with validated attributes, pseudonymous, or
1103 where appropriate, uniquely identified. Where applicable to such transactions, entities
1104 employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES
1105 collecting USER personal information. Organizations MUST request individuals' credentials only
1106 when necessary for the transaction and then only as appropriate to the risk associated with the
1107 transaction or only as appropriate to the risks to the Participants associated with the
1108 transaction.

1109

1110 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

1111 Controls on the processing or use of USERS' personal information MUST be commensurate with
1112 the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by
1113 entities who conduct digital identity management functions, to establish what risks those
1114 functions pose to USERS' privacy.

1115

1116 PRIVACY-14. DATA RETENTION AND DISPOSAL

1117 Entities MUST limit the retention of personal information to the time necessary for providing
1118 and administering the functions and services to USERS for which the information was collected,
1119 except as otherwise required by law or regulation. When no longer needed, personal
1120 information MUST be securely disposed of in a manner aligning with appropriate industry
1121 standards and/or legal requirements.

1122

1123 PRIVACY-15. ATTRIBUTE SEGREGATION

- 1124 Wherever feasible, identifier data **MUST** be segregated from attribute data.
- 1125 **SECURE-1. SECURITY PRACTICES**
- 1126 Entities **MUST** apply appropriate and industry-accepted information security **STANDARDS**,
- 1127 guidelines, and practices to the systems that support their identity functions and services.
- 1128
- 1129 **SECURE-2. DATA INTEGRITY**
- 1130 Entities **MUST** implement industry-accepted practices to protect the confidentiality and
- 1131 integrity of identity data—including authentication data and attribute values—during the
- 1132 execution of all digital identity management functions, and across the entire data lifecycle
- 1133 (collection through destruction).
- 1134
- 1135 **SECURE-3. CREDENTIAL REPRODUCTION**
- 1136 Entities that issue or manage credentials and tokens **MUST** implement industry-accepted
- 1137 processes to protect against their unauthorized disclosure and reproduction.
- 1138
- 1139 **SECURE-4. CREDENTIAL PROTECTION**
- 1140 Entities that issue or manage credentials and tokens **MUST** implement industry-accepted data
- 1141 integrity practices to enable individuals and other entities to verify the source of credential and
- 1142 token data.
- 1143
- 1144 **SECURE-5. CREDENTIAL ISSUANCE**
- 1145 Entities that issue or manage credentials and tokens **MUST** do so in a manner designed to
- 1146 assure that they are granted to the appropriate and intended **USER(s)** only. Where Registration
- 1147 and credential issuance are executed by separate entities, procedures for ensuring accurate
- 1148 exchange of Registration and issuance information that are commensurate with the stated
- 1149 assurance level **MUST** be included in business agreements and operating policies.
- 1150
- 1151 **SECURE-6. CREDENTIAL UNIQUENESS**
- 1152 Entities that issue or manage credentials **MUST** ensure that each account to credential pairing is
- 1153 uniquely identifiable within its namespace for authentication purposes.
- 1154
- 1155 **SECURE-7. TOKEN CONTROL**
- 1156 Entities that authenticate a **USER** **MUST** employ industry-accepted secure authentication
- 1157 protocols to demonstrate the **USER's** control of a valid token.
- 1158
- 1159 **SECURE-8. MULTIFACTOR AUTHENTICATION**
- 1160 Entities that authenticate a **USER** **MUST** offer authentication mechanisms which augment or are
- 1161 alternatives to a password.
- 1162
- 1163 **SECURE-9. AUTHENTICATION RISK ASSESSMENT**
- 1164 Entities **MUST** have a risk assessment process in place for the selection of authentication
- 1165 mechanisms and supporting processes.
- 1166
- 1167

1168
1169 SECURE-10. UPTIME
1170 Entities that provide and conduct digital identity management functions MUST have established
1171 policies and processes in place to maintain their stated assurances for availability of their
1172 services.
1173
1174 SECURE-11. KEY MANAGEMENT
1175 Entities that use cryptographic solutions as part of identity management MUST implement key
1176 management policies and processes that are consistent with industry-accepted practices.
1177
1178 SECURE-12. RECOVERY AND REISSUANCE
1179 Entities that issue credentials and tokens MUST implement methods for reissuance, updating,
1180 and recovery of credentials and tokens that preserve the security and assurance of the original
1181 Registration and credentialing operations.
1182
1183 SECURE-13. REVOCATION
1184 Entities that issue credentials or tokens MUST have processes and procedures in place to
1185 invalidate credentials and tokens.
1186
1187 SECURE-14. SECURITY LOGS
1188 Entities conducting digital identity management functions MUST log their transactions and
1189 security events, in a manner that supports system audits and, where necessary, security
1190 investigations and regulatory requirements. Timestamp synchronization and detail of logs
1191 MUST be appropriate to the level of risk associated with the environment and transactions.
1192
1193 SECURE-15. SECURITY AUDITS
1194 Entities MUST conduct regular audits of their compliance with their own information security
1195 policies and procedures, and any additional requirements of law, including a review of their
1196 logs, incident reports and credential loss occurrences, and MUST periodically review the
1197 effectiveness of their policies and procedures in light of that data.
1198