

# COMMONWEALTH OF VIRGINIA



## IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

### GUIDANCE DOCUMENT Digital Identity Assertions

### 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 Assertions within a Digital  
33 Identity System. References to statutes below and throughout this document shall be to the  
34 *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).<sup>1</sup>

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]<sup>2</sup> 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.

---

<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*, 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>.

- 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]<sup>3</sup>

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]<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>.

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

---

<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>.

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.<sup>5</sup>

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

---

<sup>5</sup> 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 parties 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 Assertions in a Digital Identity System. The minimum specifications have been  
579 designed to be conformant with NIST SP 800-63C.

580  
581 The document defines Assertion types, core components, presentation methods, security, and  
582 privacy provisions for Assertions. The document assumes that specific business, legal, and  
583 technical requirements for Assertions will be established in the Identity Trust Framework for  
584 each distinct Digital Identity System, and that these requirements will be designed based on the  
585 Electronic Authentication model, Identity Assurance Level (IAL), and Authenticator Assurance  
586 Level (AAL) requirements for the system.

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

591

## 592 7 Minimum Specifications

---

593

594 National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3)  
595 defines an “Assertion” in a Digital Identity System as “A statement from a verifier to a relying  
596 party (RP) that contains identity information about a Subscriber. Assertions may also contain  
597 verified attributes.”<sup>12</sup> Information Systems may use the authenticated identity to determine if  
598 that user is authorized to perform an electronic transaction.

599

600 This document establishes minimum specifications for Assertions within a Digital Identity  
601 System conformant with, and using language from, NIST SP 800-63-3. However, the minimum  
602 specifications defined in this document have been developed to accommodate requirements  
603 for Assertions established under other national and international standards.<sup>13</sup> The minimum  
604 specifications in this document also assume that specific business, legal, and technical  
605 requirements for a Digital Identity System will be documented in the Identity Trust Framework  
606 for that system. Minimum specifications for other components of a Digital Identity System have  
607 been documented in separate guidance documents in the IMSAC series, pursuant to §2.2-436  
608 and §2.2-437.

609

### 610 Electronic Authentication Model

611

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

618

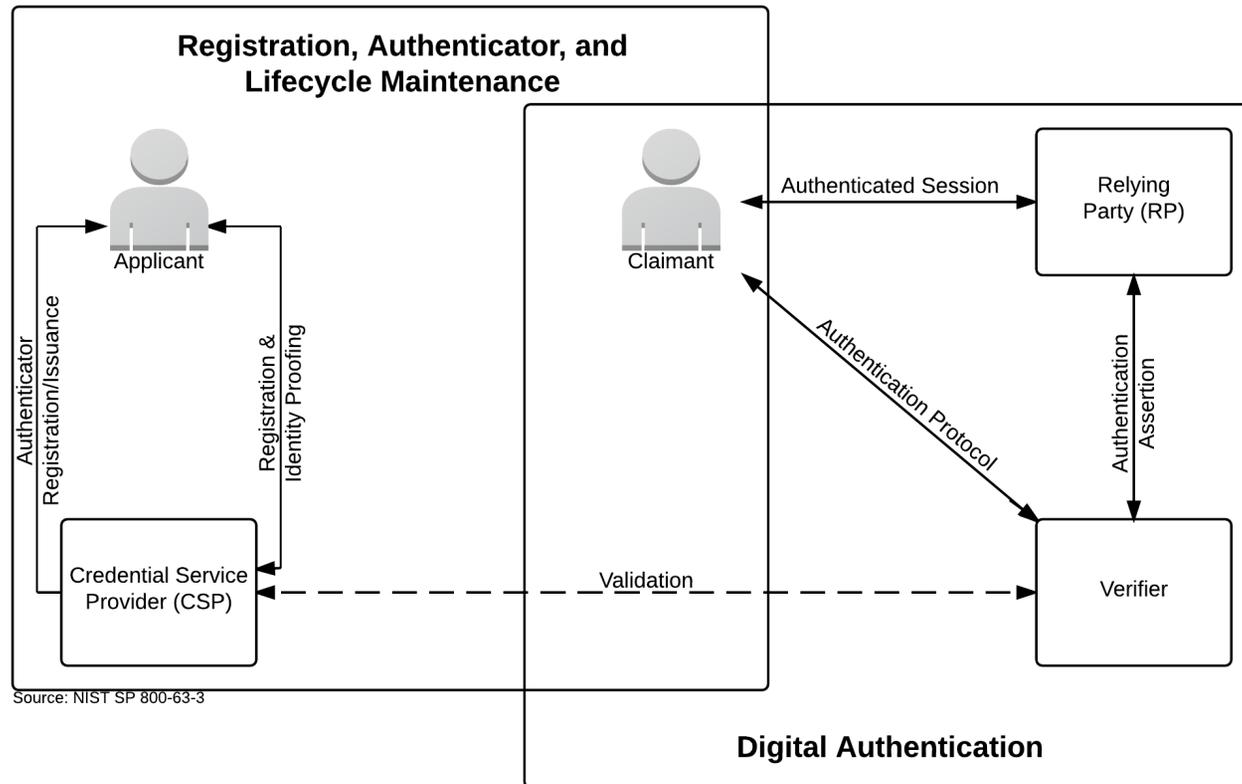
619 The minimum specifications for Assertions defined in this document reflect the Electronic  
620 Authentication model used primarily by governmental entities. More complex models that  
621 separate functions among a broader range of parties are also available and may have  
622 advantages in some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

---

<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 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>.

627 **Figure 1. Electronic Authentication Model**



628  
629  
630  
631  
632  
633  
634

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.

## 635 Assertions

636

637 An Assertion contains a set of claims or statements about an authenticated Subscriber.

638 Assertions can be categorized along multiple orthogonal dimensions, including the

639 characteristics of using the Assertion or the protections on the Assertion itself.

640

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

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

653

654 These core claims, particularly the issuance and expiration claims, apply to the Assertion about

655 the Authentication event itself, and not to any additional Identity Attributes associated with the

656 Subscriber, even when those claims are included within the Assertion. A Subscriber's Attributes

657 may expire or be otherwise invalidated independently of the expiration or invalidation of the

658 Assertion.

659

660 Assertions may include other additional Identity Attributes. Privacy requirements for presenting

661 Attributes in Assertions have been provided below in this document. The RP may fetch

662 additional Identity Attributes from the IdP in a separate transaction using an authorization

663 Credential issued alongside the Assertion.

664

665 Although details vary based on the exact Authentication or federation protocols in use, an

666 Assertion should be used only to represent a single log-in event at the RP. After the RP

667 consumes the Assertion, session management at the RP comes into play and the Assertion is no

668 longer used directly. The expiration of the Assertion must not represent the expiration of the

669 session at the RP.

670

### 671 Assertion Possession Category

672 An Assertion can be classified based on whether possession of the Assertion itself is sufficient

673 for representing the subject of the Assertion, or if additional proof is necessary alongside the

674 Assertion.

675

676

677

## 678 Holder-of-Key Assertions

679 A Holder-of-Key Assertion contains a reference to a Symmetric Key or a Public Key  
680 (corresponding to a Private Key) possessed by and representing the Subscriber. An RP may  
681 decide when to require the Subscriber to prove possession of the key, depending on the policy  
682 of the RP. However, the RP must require the Subscriber to prove possession of the key that is  
683 referenced in the Assertion in parallel with presentation of the Assertion itself in order for the  
684 Assertion to be considered Holder-Of-Key. Otherwise, an Assertion containing reference to a  
685 key which the user has not proved possession of will be considered a Bearer Assertion.

686  
687 The key referenced in a Holder-of-Key represents the Subscriber, not the client. This key may be  
688 distinct from any key used by the Subscriber to Authenticate to the IdP. In proving possession  
689 of the Subscriber's secret, the Subscriber also proves with a certain degree of assurance that  
690 they are the rightful subject of the Assertion. It is more difficult for an attacker to use a stolen  
691 Holder-of-Key Assertion issued to a Subscriber, since the attacker would need to steal the  
692 referenced key material as well.

693  
694 Note that the reference to the key material in question is asserted by the issuer of the Assertion  
695 as are any other claims therein, and reference to a given key must be trusted at the same level  
696 as all other claims within the Assertion itself. The Assertion must not include an unencrypted  
697 Private or Symmetric Key to be used with Holder-of-Key presentation.

## 698 Bearer Assertions

699 A bearer Assertion can be presented by any party as proof of the bearer's identity, without  
700 reference to external materials. If an attacker is able to capture or manufacture a valid  
701 Assertion representing a Subscriber, and that attacker is able to successfully present that  
702 Assertion to the RP, then the attacker will be able to impersonate the Subscriber at that RP.

703  
704  
705 Note that mere possession of a bearer Assertion is not always enough to impersonate a  
706 Subscriber. For example, if an Assertion is presented in the indirect federation model (Section  
707 6.1), additional controls may be placed on the transaction (such as identification of the RP and  
708 Assertion injection protections) that help to further protect the RP from fraudulent activity.

## 709 Assertion Protection Category

710  
711  
712 Regardless of the possession mechanism used to obtain them, Assertions must include an  
713 appropriate set of protections to the Assertion data itself to prevent attackers from  
714 manufacturing valid Assertions or re-using captured Assertions at disparate RPs.

## 715 Assertion Identifier

716  
717 Assertions must contain sufficient Entropy to prevent an attacker from manufacturing a valid  
718 Assertion and using it with a target RP. Assertions may accomplish this by use of an embedded  
719 Nonce, timestamp, Assertion identifier, or a combination of these or other techniques. In the  
720 absence of additional Cryptographic protections, this source of randomness must function as a  
721 shared secret between the IdP and the RP to uniquely identify the Assertion in question.

## 722 Signed Assertion

723 Assertions may be Cryptographically signed by the IdP, and the RP must validate the signature  
724 of each such Assertion based on the IdP's key. This signature must cover all vital fields of the  
725 Assertion, including its issuer, audience, subject, expiration, and any unique identifiers.

726

727 The signature may be asymmetric based on the published Public Key of the IdP. In such cases,  
728 the RP may fetch this Public Key in a secure fashion at runtime (such as through an HTTPS URL  
729 hosted by the IdP), or the key may be provisioned out of band at the RP (during configuration of  
730 the RP). The signature may be symmetric based on a key shared out of band between the IdP  
731 and the RP. In such circumstances, the IdP must use a different shared key for each RP. All  
732 signatures must use approved signing methods.

733

## 734 Encrypted Assertion

735 Assertions may be encrypted in such a fashion as to allow only the intended audience to  
736 decrypt the claims therein. The IdP must encrypt the payload of the Assertion using the RP's  
737 Public Key. The IdP may fetch this Public Key in a secure fashion at runtime (such as through an  
738 HTTPS URL hosted by the RP), or the key may be provisioned out of band at the IdP (during  
739 registration of the RP). All encrypted objects must use approved encryption methods.

740

## 741 Audience Restriction

742 All Assertions should use audience restriction techniques to allow an RP to recognize whether  
743 or not it is the intended target of an issued Assertion. All RPs must check the audience of an  
744 Assertion, if provided, to prevent the injection and replay of an Assertion generated for one RP  
745 at another RP.

746

## 747 Pairwise Pseudonymous Identifiers

748 In some circumstances, it is desirable to prevent the Subscriber's account at the IdP from being  
749 linked through one or more RPs through use of a common identifier. In these circumstances,  
750 pairwise Pseudonymous Identifiers must be used within the Assertions generated by the IdP for  
751 the RP, and the IdP must generate a different identifier for each RP. (See Pairwise  
752 Pseudonymous Identifier Generation for more information.)

753

754 When unique Pseudonymous Identifiers are used with RPs alongside of Identity Attribute  
755 bundles, it may still be possible for multiple colluding RPs to fully identify and correlate a  
756 Subscriber across Digital Identity Systems using these attributes. For example, given that two  
757 independent RPs will each see the same Subscriber identified with a different pairwise  
758 Pseudonymous Identifier, the RPs could still determine that the Subscriber is the same person  
759 by comparing their name, email address, Physical Address, or other identifying Attributes  
760 carried alongside the pairwise Pseudonymous Identifier. Privacy policies may prohibit such  
761 correlation, but pairwise Pseudonymous Identifiers can increase effectiveness of these policies  
762 by increasing the administrative effort in managing the Attribute correlation.

763

764

765 Note that in a proxied federation model, ultimate IdP may be unable to generate a pairwise  
766 Pseudonymous Identifier for the ultimate RP, since the proxy could blind the IdP from knowing  
767 which RP is being accessed by the Subscriber. In such situations, the pairwise Pseudonymous  
768 Identifier is usually between the IdP and the federation proxy itself. The proxy, acting as an IdP,  
769 can itself provide pairwise Pseudonymous Identifiers to downstream RPs. Depending on the  
770 protocol, the federation proxy may need to map the pairwise Pseudonymous Identifiers back to  
771 the associated identifiers from upstream IdPs in order to allow the Identity protocol to function.  
772 In such cases, the proxy will be able to track and determine which pairwise Pseudonymous  
773 Identifiers represent the same Subscriber at different RPs.

#### 774 Pairwise Pseudonymous Identifier Generation

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

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

783  
784 The RPs must conduct a privacy risk assessment to consider the privacy risks associated with  
785 requesting a common identifier. The IdP must ensure that only intended RPs are correlated;  
786 otherwise, a rogue RP could learn of the Pseudonymous Identifier for a correlation by  
787 fraudulently posing as part of that correlation.

#### 788 Assertion Presentation

789  
790  
791 Assertions may be presented in either a back-channel or front-channel manner from the IdP to  
792 the RP. Each model has its benefits and drawbacks, but both require the proper validation of  
793 the Assertion. Assertions may also be proxied to facilitate federation between IdPs and RPs  
794 under specific circumstances. The IdP must transmit only those Attributes that were explicitly  
795 requested by the RP. RPs must conduct a privacy risk assessment when determining which  
796 attributes to request.

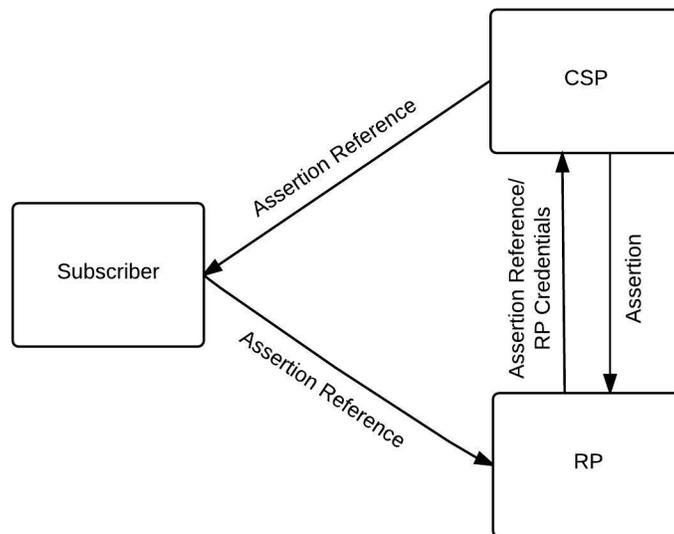
797  
798 The Subscriber must be able to view the Attribute values to be transmitted, although masking  
799 mechanisms must be employed, as necessary, to mitigate the risk of unauthorized exposure of  
800 sensitive information (e.g. shoulder surfing). The Subscriber must receive explicit notice and be  
801 able to provide positive confirmation before any attributes about the Subscriber are  
802 transmitted to any RP.

803  
804 At a minimum, the notice should be provided by the party in the position to provide the most  
805 effective notice and obtain confirmation. If the protocol in use allows for optional Attributes,  
806 the Subscriber must be given the option to decide whether to transmit those Attributes to the  
807 RP. A IdP may employ mechanisms to remember and re-transmit the exact Attribute bundle to  
808 the same RP.

809 Back-Channel Presentation

810 In the back-channel model, the Subscriber is given an Assertion reference to present to the RP,  
 811 generally through the front channel. The Assertion reference itself contains no information  
 812 about the Subscriber and must be resistant to tampering and fabrication by an attacker. The RP  
 813 presents the Assertion reference to the IdP, usually along with authentication of the RP itself, to  
 814 fetch the Assertion. **Figure 2** shows the back-channel presentation model.

815  
 816 **Figure 2. Back-Channel Assertion Presentation**



Source: NIST SP 800-63C

817  
 818  
 819 In the back-channel model, the Assertion itself is requested directly from the IdP to the RP,  
 820 minimizing chances of interception and manipulation by a third party (including the Subscriber  
 821 themselves). This method also allows the RP to query the CSP for additional attributes about  
 822 the Subscriber not included in the Assertion itself, since back-channel communication can  
 823 continue to occur after the initial authentication transaction has completed.

824  
 825 The back-channel method also requires more network transactions than the front-channel  
 826 model, but the information is limited to the only required parties. Since an RP is expecting to  
 827 get an Assertion only from the IdP directly, the attack surface is reduced since it is more difficult  
 828 to inject Assertions directly into the RP.

829  
 830 The Assertion Reference:

- 831 • Must be limited to use by a single RP
- 832 • Must be single-use
- 833 • Should be time limited with a short lifetime of seconds or minutes
- 834 • Should be presented along with authentication of the RP

835 The RP must protect itself against injection of manufactured or captured Assertion references  
 836 by use of cross-site scripting protection or other accepted techniques. Claims within the  
 837 Assertion must be validated including issuer verification, signature validation, and audience  
 838 restriction.

839

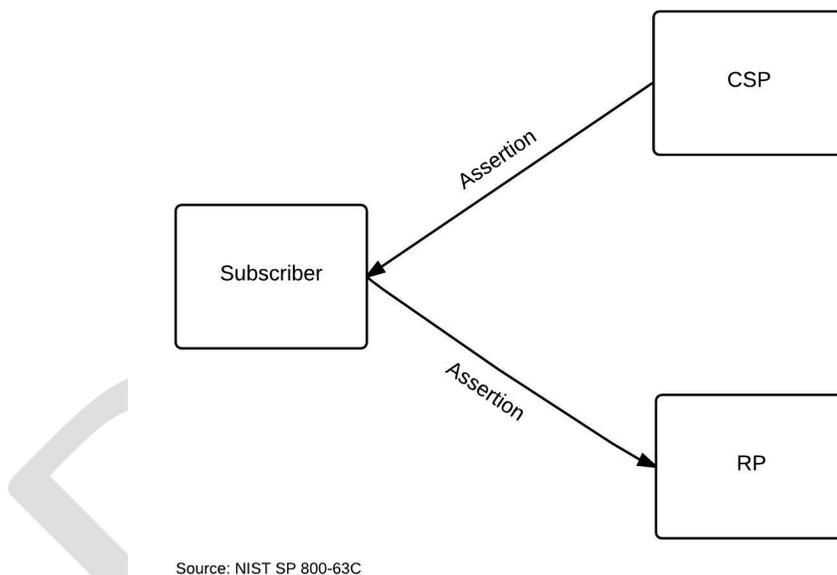
840 Conveyance of the Assertion reference from the IdP to the Subscriber as well as from the  
 841 Subscriber to the RP must be made over an authenticated protected channel. Conveyance of  
 842 the Assertion reference from the RP to the IdP as well as the Assertion from the IdP to the RP  
 843 must be made over an authenticated protected channel. Presentation of the Assertion  
 844 reference at the IdP should require Authentication of the RP before issuance of an Assertion.  
 845

846 **Front-Channel Presentation**

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

851

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



853

854

855 In the front-channel method, an Assertion is visible to the Subscriber, which could potentially  
 856 cause leakage of system information included in the Assertion. Since the Assertion is under the  
 857 control of the Subscriber, the front-channel presentation method also allows the Subscriber to  
 858 submit a single Assertion to unintended parties, perhaps by a browser replaying an Assertion at  
 859 multiple RPs. Even if the Assertion is audience restricted and rejected by RPs, its presentation at  
 860 unintended RPs could lead to leaking information about the Subscriber and their online  
 861 activities.

862

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

867

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

873

#### 874 Assertion Proxying

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

879

880 There are several common reasons for such proxies:

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

886

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

888

#### 889 Assertion Security

890

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

896

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

901

902 Common attacks against Assertion transmission transactions include the following:

- 903 • Assertion Manufacture/Modification: An attacker generates a forged Assertion or  
904 modifies the content of an existing Assertion (such as the authentication or attribute  
905 statements), causing the RP to grant inappropriate access to the Subscriber. For

906 example, an attacker may modify the Assertion to extend the validity period and keep  
907 using an Assertion; or a Subscriber may modify the Assertion to have access to  
908 information that they should not be able to view.

- 909 • Assertion Disclosure: Assertions may contain authentication and attribute statements  
910 that include sensitive Subscriber information. Disclosure of the Assertion contents can  
911 make the Subscriber vulnerable to other types of attacks.
- 912 • Assertion Repudiation by the IdP: An Assertion may be repudiated by an IdP if the  
913 proper mechanisms are not in place. For example, if an IdP does not digitally sign an  
914 Assertion, the IdP can claim that it was not generated through the services of the IdP.
- 915 • Assertion Repudiation by the Subscriber: Since it is possible for a compromised or  
916 malicious IdP to issue Assertions to the wrong party, a Subscriber can repudiate any  
917 transaction with the RP that was authenticated using only a bearer Assertion.
- 918 • Assertion Redirect: An attacker uses the Assertion generated for one RP to obtain access  
919 to a second RP.
- 920 • Assertion Reuse: An attacker attempts to use an Assertion that has already been used  
921 once with the intended RP.

922

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

927

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

933

934 Threats to the secondary authenticator include the following:

- 935 • Secondary Authenticator Manufacture: An attacker may attempt to generate a valid  
936 secondary authenticator and use it to impersonate a Subscriber.
- 937 • Secondary Authenticator Capture: An attacker may use a session hijacking attack to  
938 capture the secondary authenticator when the IdP transmits it to the Subscriber after  
939 the primary authentication step, or the attacker may use a man-in-the-middle attack to  
940 obtain the secondary authenticator as it is being used by the Subscriber to authenticate  
941 to the RP. If, as in the indirect model, the RP needs to send the secondary authenticator  
942 back to the IdP in order to check its validity or obtain the corresponding Assertion data,  
943 an attacker may similarly subvert the communication protocol between the IdP and the  
944 RP to capture a secondary authenticator. In any of the above scenarios, the secondary  
945 authenticator can be used to impersonate the Subscriber.

946

947

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

954

#### 955 Threat Mitigation Strategies

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

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

986

- 987
- Assertion Reuse: To mitigate this threat, the following mechanisms are used:
    - The Assertion includes a timestamp and has a short lifetime of validity. The RP checks the timestamp and lifetime values to ensure the Assertion is currently valid.
    - The RP keeps track of Assertions that were consumed within a (configurable) time window to ensure that an Assertion is not used more than once within that time window.
  - Secondary Authenticator Manufacture: To mitigate this threat, one of the following mechanisms is used:
    - The secondary authenticator may contain sufficient entropy that an attacker without direct access to the IdP's random number generator cannot guess the value of a valid secondary authenticator.
    - The secondary authenticator may contain timely Assertion data that is signed by the IdP or integrity protected using a key shared between the IdP and the RP.
  - Secondary Authenticator Capture: To mitigate this threat, adequate protections are in place throughout the lifetime of any secondary authenticators used in the Assertion protocol:
    - In order to protect the secondary authenticator while it is in transit between the IdP and the Subscriber, the secondary authenticator is sent via a protected session established during the primary authentication of the Subscriber.
    - In order to protect the secondary authenticator from capture as it is submitted to the RP, the secondary authenticator is used in an authentication protocol which protects against eavesdropping and man-in-the-middle attacks.
    - In order to protect the secondary authenticator after it has been used, it is never transmitted over an unprotected session or to an unauthenticated party while it is still valid.
  - Assertion Substitution: To mitigate this threat, one of the following mechanisms is used:
    - Responses to Assertion requests contain the value of the Assertion reference used in the request or some other nonce that was cryptographically bound to the request by the RP.
    - Responses to Assertion requests are bound to the corresponding requests by message order, as in HTTP, provided that Assertions and requests are protected by a protocol such as TLS that can detect and disallow malicious reordering of packets.

## 1020 Assertion Examples

1021

1022 The following represent three (3) types of Assertion technologies: Security Assertion Markup  
1023 Language (SAML) Assertions, Kerberos tickets, and OpenID Connect tokens.

1024

### 1025 Security Assertion Markup Language (SAML)

1026 SAML is an XML-based framework for creating and exchanging authentication and Attribute  
1027 information between trusted entities over the internet. As of this writing, the latest  
1028 specification for [SAML] is SAML v2.0, issued 15 March 2005.

1029 The building blocks of SAML include:

- 1030 • Assertion XML schema which defines the structure of the Assertion
- 1031 • SAML Protocols which are used to request Assertions and artifacts
- 1032 • Bindings that define the underlying communication protocols (such as HTTP or SOAP)
- 1033 and can be used to transport the SAML Assertions.

1034

1035 The three components above define a SAML profile that corresponds to a particular use case  
1036 such as “Web Browser SSO.” SAML Assertions are encoded in an XML schema and can carry up  
1037 to three types of statements:

- 1038 • Authentication statements include information about the Assertion issuer, the  
1039 authenticated Subscriber, validity period, and other authentication information. For  
1040 example, an Authentication Assertion would state the Subscriber “John” was  
1041 authenticated using a password at 10:32 p.m. on 06-06-2004.
- 1042 • Attribute statements contain specific additional characteristics related to the  
1043 Subscriber. For example, subject “John” is associated with attribute “Role” with value  
1044 “Manager.”
- 1045 • Authorization statements identify the resources the Subscriber has permission to  
1046 access. These resources may include specific devices, files, and information on specific  
1047 web servers. For example, subject “John” for action “Read” on “Webserver1002” given  
1048 evidence “Role.”

1049

#### 1050 Kerberos Tickets

1051 The Kerberos Network Authentication Service [RFC 4120] was designed to provide strong  
1052 authentication for client/server applications using symmetric-key cryptography on a local,  
1053 shared network. Extensions to Kerberos can support the use of public key cryptography for  
1054 selected steps of the protocol. Kerberos also supports confidentiality and integrity protection of  
1055 session data between the Subscriber and the RP. Even though Kerberos uses Assertions, since it  
1056 is designed for use on shared networks it is not truly a federation protocol.

1057

1058 Kerberos supports authentication of a Subscriber over an untrusted, shared local network using  
1059 one or more IdPs. The Subscriber implicitly authenticates to the IdP by demonstrating the  
1060 ability to decrypt a random session key encrypted for the Subscriber by the IdP. (Some Kerberos  
1061 variants also require the Subscriber to explicitly authenticate to the IdP, but this is not  
1062 universal.)

1063

1064 In addition to the encrypted session key, the IdP also generates another encrypted object called  
1065 a Kerberos ticket. The ticket contains the same session key, the identity of the Subscriber to  
1066 whom the session key was issued, and an expiration time after which the session key is no  
1067 longer valid. The ticket is confidentiality and integrity protected by a pre-established that is key  
1068 shared between the IdP and the RP during an explicit setup phase.

1069

1070 To authenticate using the session key, the Subscriber sends the ticket to the RP along with  
1071 encrypted data that proves that the Subscriber possesses the session key embedded within the

1072 Kerberos ticket. Session keys are either used to generate new tickets, or to encrypt and  
1073 authenticate communications between the Subscriber and the RP.

1074

1075 To begin the process, the Subscriber sends an authentication request to the Authentication  
1076 Server (AS). The AS encrypts a session key for the Subscriber using the Subscriber's long term  
1077 Credential. The long term Credential may either be a secret key shared between the AS and the  
1078 Subscriber, or in the PKINIT variant of Kerberos, a Public Key Certificate. It should be noted that  
1079 most variants of Kerberos based on a Shared Secret key between the Subscriber and IdP derive  
1080 this key from a user generated password. As such, they are vulnerable to offline dictionary  
1081 attack by a passive eavesdropper.

1082

1083 In addition to delivering the session key to the Subscriber, the AS also issues a ticket using a key  
1084 it shares with the Ticket Granting Server (TGS). This ticket is referred to as a Ticket Granting  
1085 Ticket (TGT), since the verifier uses the session key in the TGT to issue tickets rather than to  
1086 explicitly authenticate the verifier. The TGS uses the session key in the TGT to encrypt a new  
1087 session key for the Subscriber and uses a key it shares with the RP to generate a ticket  
1088 corresponding to the new session key. The Subscriber decrypts the session key and uses the  
1089 ticket and the new session key together to authenticate to the RP.

1090

1091 OpenID Connect

1092 OpenID Connect is an internet-scale federated identity and authentication protocol built on top  
1093 of the OAuth 2.0 authorization framework and the JSON Object Signing and Encryption (JOSE)  
1094 cryptographic system. As of this writing, the latest specification is version 1.0 with errata, dated  
1095 November 8, 2014.

1096

1097 OpenID Connect builds on top of the OAuth 2.0 authorization protocol to enable the Subscriber  
1098 to authorize the RP to access the Subscriber's identity and authentication information. The RP  
1099 in both OpenID Connect and OAuth 2.0 is known as the client.

1100

1101 In a successful OpenID Connect transaction, the IdP issues an ID Token, which is a signed  
1102 Assertion in JSON Web Token (JWT) format. The client parses the ID Token to learn about the  
1103 Subscriber and primary authentication event at the IdP. This token contains at minimum the  
1104 following claims about the Subscriber and authentication event:

- 1105 • **iss** : HTTPS URL identifying the IdP that issued the Assertion
- 1106 • **sub** : IdP-specific subject identifier representing the Subscriber
- 1107 • **aud** : IdP-specific audience identifier, equal to the OAuth 2.0 client identifier of the client  
1108 at the IdP
- 1109 • **exp** : Timestamp at which the Identity token expires and after which must not be  
1110 accepted the client
- 1111 • **iat** : Timestamp at which the Identity token was issued and before which must not be  
1112 accepted by the client

1113

1114

1115 In addition to the Identity token, the IdP also issues the client an OAuth 2.0 access token which  
1116 can be used to access the UserInfo Endpoint at the IdP. This endpoint returns a JSON object  
1117 representing a set of claims about the Subscriber, including but not limited to their name, email  
1118 address, physical address, phone number, and other profile information.

1119

1120 While the information inside the ID Token is reflective of the authentication event, the  
1121 information in the UserInfo Endpoint is generally more stable and could be more general  
1122 purpose. Access to different claims from the UserInfo Endpoint is governed by the use of a  
1123 specially defined set of OAuth scopes, `openid`, `profile`, `email`, `phone`, and `address`. An  
1124 additional scope, `offline_access`, is used to govern the issuance of refresh tokens, which  
1125 allow the RP to access the UserInfo Endpoint when the Subscriber is not present.

DRAFT

## 1127 Privacy and Security

1128

1129 The minimum specifications established in this document for privacy and security in the use of  
1130 person information for Electronic Authentication apply the Fair Information Practice Principles  
1131 (FIPPs).<sup>16</sup> The FIPPs have been endorsed by the National Strategy for Trusted Identities in  
1132 Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.<sup>17</sup>

1133

1134 The minimum specifications also adhere to the Identity Ecosystem Framework (IDEF) Baseline  
1135 Functional Requirements (v.1.0) for privacy and security, adopted by the Identity Ecosystem  
1136 Steering Group (IDESG) in October 2015 (**Appendix 2**).

1137

1138 The minimum specifications for Assertions apply the following FIPPs:

- 1139 • Transparency: RAs and CSPs should be transparent and provide notice to Applicants  
1140 regarding collection, use, dissemination, and maintenance of person information required  
1141 during the Registration, Identity Proofing and verification processes.
- 1142 • Individual Participation: RAs and CSPs should involve the Applicant in the process of using  
1143 person information and, to the extent practicable, seek consent for the collection, use,  
1144 dissemination, and maintenance of that information. RAs and CSPs also should provide  
1145 mechanisms for appropriate access, correction, and redress of person information.
- 1146 • Purpose Specification: RAs and CSPs should specifically articulate the authority that permits  
1147 the collection of person information and specifically articulate the purpose or purposes for  
1148 which the information is intended to be used.
- 1149 • Data Minimization: RAs and CSPs should collect only the person information directly  
1150 relevant and necessary to accomplish the Registration and related processes, and only  
1151 retain that information for as long as necessary to fulfill the specified purpose.
- 1152 • Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for  
1153 the purpose specified in the notice. Disclosure or sharing that information should be limited  
1154 to the specific purpose for which the information was collected.
- 1155 • Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that  
1156 person information is accurate, relevant, timely, and complete.
- 1157 • Security: RAs and CSPs should protect personal information through appropriate security  
1158 safeguards against risks such as loss, unauthorized access or use, destruction, modification,  
1159 or unintended or inappropriate disclosure.
- 1160 • Accountability and Auditing: RAs and CSPs should be accountable for complying with these  
1161 principles, providing training to all employees and contractors who use person information,  
1162 and auditing the actual use of person information to demonstrate compliance with these  
1163 principles and all applicable privacy protection requirements.

---

<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 Identity Trust Framework for the 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>.

## 1164 Appendix 1. IMSAC Charter

1165

1166

1167

1168

1169

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

1170 **Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)**

1171

1172 The Identity Management Standards Advisory Council (the Advisory Council) advises the  
1173 Secretary of Technology on the adoption of identity management standards and the creation of  
1174 guidance documents pursuant to § 2.2-436.

1175

1176 The Advisory Council recommends to the Secretary of Technology guidance documents relating  
1177 to (i) nationally recognized technical and data standards regarding the verification and  
1178 authentication of identity in digital and online transactions; (ii) the minimum specifications and  
1179 standards that should be included in an Identity Trust Framework, as defined in § 59.1-550, so  
1180 as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-  
1181 550 et seq.); and (iii) any other related data standards or specifications concerning reliance by  
1182 third parties on identity credentials, as defined in § 59.1-550.

1183

1184 **Membership and Governance Structure (§ 2.2-437.B)**

1185

1186 The Advisory Council's membership and governance structure is as follows:

1187 1. The Advisory Council consists of seven members, to be appointed by the Governor, with  
1188 expertise in electronic identity management and information technology. Members include  
1189 a representative of the Department of Motor Vehicles, a representative of the Virginia  
1190 Information Technologies Agency, and five representatives of the business community with  
1191 appropriate experience and expertise. In addition to the seven appointed members, the  
1192 Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex  
1193 officio member of the Advisory Council.

1194

1195 2. The Advisory Council designates one of its members as chairman.

1196

1197 3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure  
1198 of the Governor, and may be reappointed.

1199

1200 4. Members serve without compensation but may be reimbursed for all reasonable and  
1201 necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

1202

1203 5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

1204

1205

1206 The formation, membership and governance structure for the Advisory Council has been  
1207 codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

1208

1209 The statutory authority and requirements for public notice and comment periods for guidance  
1210 documents have been established pursuant to § 2.2-437.C, as follows:

1211

1212 C. Proposed guidance documents and general opportunity for oral or written submittals as to  
1213 those guidance documents shall be posted on the Virginia Regulatory Town Hall and published  
1214 in the Virginia Register of Regulations as a general notice following the processes and  
1215 procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§  
1216 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written  
1217 comments following the posting and publication and shall hold at least one meeting dedicated  
1218 to the receipt of oral comment no less than 15 days after the posting and publication. The  
1219 Advisory Council shall also develop methods for the identification and notification of interested  
1220 parties and specific means of seeking input from interested persons and groups. The Advisory  
1221 Council shall send a copy of such notices, comments, and other background material relative to  
1222 the development of the recommended guidance documents to the Joint Commission on  
1223 Administrative Rules.

1224

1225

1226 This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the  
1227 minutes of the meeting and related IMSAC documents, visit:  
1228 <https://vita.virginia.gov/About/default.aspx?id=6442474173>

1229 Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline  
1230 Functional Requirements (v.1.0) for Privacy and Security

1231

1232 PRIVACY-1. DATA MINIMIZATION

1233 Entities MUST limit the collection, use, transmission and storage of personal information to the  
1234 minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities  
1235 providing claims or attributes MUST NOT provide any more personal information than what is  
1236 requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to  
1237 accommodate information requests of variable granularity, to support data minimization.

1238

1239 PRIVACY-2. PURPOSE LIMITATION

1240 Entities MUST limit the use of personal information that is collected, used, transmitted, or  
1241 stored to the specified purposes of that transaction. Persistent records of contracts, assurances,  
1242 consent, or legal authority MUST be established by entities collecting, generating, using,  
1243 transmitting, or storing personal information, so that the information, consistently is used in  
1244 the same manner originally specified and permitted.

1245

1246 PRIVACY-3. ATTRIBUTE MINIMIZATION

1247 Entities requesting attributes MUST evaluate the need to collect specific attributes in a  
1248 transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST  
1249 collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever  
1250 feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities  
1251 MUST be bound to claims instead of actual attribute values.

1252

1253 PRIVACY-4. CREDENTIAL LIMITATION

1254 Entities MUST NOT request USERS' credentials unless necessary for the transaction and then  
1255 only as appropriate to the risk associated with the transaction or to the risks to the parties  
1256 associated with the transaction.

1257

1258 PRIVACY-5. DATA AGGREGATION RISK

1259 Entities MUST assess the privacy risk of aggregating personal information, in systems and  
1260 processes where it is collected, generated, used, transmitted, or stored, and wherever feasible,  
1261 MUST design and operate their systems and processes to minimize that risk. Entities MUST  
1262 assess and limit linkages of personal information across multiple transactions without the  
1263 USER's explicit consent.

1264

1265 PRIVACY-6. USAGE NOTICE

1266 Entities MUST provide concise, meaningful, and timely communication to USERS describing how  
1267 they collect, generate, use, transmit, and store personal information.

1268

1269 PRIVACY-7. USER DATA CONTROL

1270 Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete  
1271 personal information.

## 1272 PRIVACY-8. THIRD-PARTY LIMITATIONS

1273 Wherever USERS make choices regarding the treatment of their personal information, those  
1274 choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it  
1275 transmits the personal information.

1276

## 1277 PRIVACY-9. USER NOTICE OF CHANGES

1278 Entities MUST, upon any material changes to a service or process that affects the prior or  
1279 ongoing collection, generation, use, transmission, or storage of USERS' personal information,  
1280 notify those USERS, and provide them with compensating controls designed to mitigate privacy  
1281 risks that may arise from those changes, which may include seeking express affirmative consent  
1282 of USERS in accordance with relevant law or regulation.

1283

## 1284 PRIVACY-10. USER OPTION TO DECLINE

1285 USERS MUST have the opportunity to decline Registration; decline credential provisioning;  
1286 decline the presentation of their credentials; and decline release of their attributes or claims.

1287

## 1288 PRIVACY-11. OPTIONAL INFORMATION

1289 Entities MUST clearly indicate to USERS what personal information is mandatory and what  
1290 information is optional prior to the transaction.

1291

## 1292 PRIVACY-12. ANONYMITY

1293 Wherever feasible, entities MUST utilize identity systems and processes that enable  
1294 transactions that are anonymous, anonymous with validated attributes, pseudonymous, or  
1295 where appropriate, uniquely identified. Where applicable to such transactions, entities  
1296 employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES  
1297 collecting USER personal information. Organizations MUST request individuals' credentials only  
1298 when necessary for the transaction and then only as appropriate to the risk associated with the  
1299 transaction or only as appropriate to the risks to the parties associated with the transaction.

1300

## 1301 PRIVACY-13. CONTROLS PROPORTIONATE TO RISK

1302 Controls on the processing or use of USERS' personal information MUST be commensurate with  
1303 the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by  
1304 entities who conduct digital identity management functions, to establish what risks those  
1305 functions pose to USERS' privacy.

1306

## 1307 PRIVACY-14. DATA RETENTION AND DISPOSAL

1308 Entities MUST limit the retention of personal information to the time necessary for providing  
1309 and administering the functions and services to USERS for which the information was collected,  
1310 except as otherwise required by law or regulation. When no longer needed, personal  
1311 information MUST be securely disposed of in a manner aligning with appropriate industry  
1312 standards and/or legal requirements.

1313

## 1314 PRIVACY-15. ATTRIBUTE SEGREGATION

1315 Wherever feasible, identifier data MUST be segregated from attribute data.

## 1316 SECURE-1. SECURITY PRACTICES

1317 Entities MUST apply appropriate and industry-accepted information security STANDARDS,  
1318 guidelines, and practices to the systems that support their identity functions and services.

1319

## 1320 SECURE-2. DATA INTEGRITY

1321 Entities MUST implement industry-accepted practices to protect the confidentiality and  
1322 integrity of identity data—including authentication data and attribute values—during the  
1323 execution of all digital identity management functions, and across the entire data lifecycle  
1324 (collection through destruction).

1325

## 1326 SECURE-3. CREDENTIAL REPRODUCTION

1327 Entities that issue or manage credentials and tokens MUST implement industry-accepted  
1328 processes to protect against their unauthorized disclosure and reproduction.

1329

## 1330 SECURE-4. CREDENTIAL PROTECTION

1331 Entities that issue or manage credentials and tokens MUST implement industry-accepted data  
1332 integrity practices to enable individuals and other entities to verify the source of credential and  
1333 token data.

1334

## 1335 SECURE-5. CREDENTIAL ISSUANCE

1336 Entities that issue or manage credentials and tokens MUST do so in a manner designed to  
1337 assure that they are granted to the appropriate and intended USER(s) only. Where Registration  
1338 and credential issuance are executed by separate entities, procedures for ensuring accurate  
1339 exchange of Registration and issuance information that are commensurate with the stated  
1340 assurance level MUST be included in business agreements and operating policies.

1341

## 1342 SECURE-6. CREDENTIAL UNIQUENESS

1343 Entities that issue or manage credentials MUST ensure that each account to credential pairing is  
1344 uniquely identifiable within its namespace for authentication purposes.

1345

## 1346 SECURE-7. TOKEN CONTROL

1347 Entities that authenticate a USER MUST employ industry-accepted secure authentication  
1348 protocols to demonstrate the USER's control of a valid token.

1349

## 1350 SECURE-8. MULTIFACTOR AUTHENTICATION

1351 Entities that authenticate a USER MUST offer authentication mechanisms which augment or are  
1352 alternatives to a password.

1353

## 1354 SECURE-9. AUTHENTICATION RISK ASSESSMENT

1355 Entities MUST have a risk assessment process in place for the selection of authentication  
1356 mechanisms and supporting processes.

1357

1358

1359

## 1360 SECURE-10. UPTIME

1361 Entities that provide and conduct digital identity management functions MUST have established  
1362 policies and processes in place to maintain their stated assurances for availability of their  
1363 services.

1364

## 1365 SECURE-11. KEY MANAGEMENT

1366 Entities that use cryptographic solutions as part of identity management MUST implement key  
1367 management policies and processes that are consistent with industry-accepted practices.

1368

## 1369 SECURE-12. RECOVERY AND REISSUANCE

1370 Entities that issue credentials and tokens MUST implement methods for reissuance, updating,  
1371 and recovery of credentials and tokens that preserve the security and assurance of the original  
1372 Registration and credentialing operations.

1373

## 1374 SECURE-13. REVOCATION

1375 Entities that issue credentials or tokens MUST have processes and procedures in place to  
1376 invalidate credentials and tokens.

1377

## 1378 SECURE-14. SECURITY LOGS

1379 Entities conducting digital identity management functions MUST log their transactions and  
1380 security events, in a manner that supports system audits and, where necessary, security  
1381 investigations and regulatory requirements. Timestamp synchronization and detail of logs  
1382 MUST be appropriate to the level of risk associated with the environment and transactions.

1383

## 1384 SECURE-15. SECURITY AUDITS

1385 Entities MUST conduct regular audits of their compliance with their own information security  
1386 policies and procedures, and any additional requirements of law, including a review of their  
1387 logs, incident reports and credential loss occurrences, and MUST periodically review the  
1388 effectiveness of their policies and procedures in light of that data.

1389