

COMMONWEALTH OF VIRGINIA



~~Information Technology Resource
Management~~ **IDENTITY MANAGEMENT STANDARDS
ADVISORY COUNCIL (ITRMIMSAC)**

REFERENCE DOCUMENT:
Terminology and Definitions

~~Virginia Information Technologies Agency (VITA)~~

1 Background

In 2015, Virginia’s General Assembly passed the Electronic Identity Management Act (Chapter 50 of Title 59.1, Code of Virginia) to address demand in the state’s digital economy for secure, privacy enhancing ~~electronic authentication~~ digital authentication and identity management. Growing numbers of “communities of interest” have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers, verifiers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly also created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents, pursuant to § 2.2-436.

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

This document establishes a standards-based terminology and definitions for core concepts in the digital identity management domain, as applied in the IMSAC guidance document series. The IMSAC terminology satisfies three primary requirements for the Commonwealth’s minimum specification: (1) aligns with the National Institute of Standards and Technology Special Publication 800-63-3, which sets federal guidelines for digital authentication and identity management; (2) complies with terminology codified under the Electronic Identity Management Act (§ 59.1-550); and (3) remains consistent with terminology published by standards development organizations (SDOs) in the global identity ecosystem.

The IMSAC terminology consists of the following definition sets:

- National Institute of Standards and Technology Special Publication 800-63-3
<https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3>
- Electronic Identity Management Act, § 59.1-550. Definitions, *Code of Virginia*
<http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/>
- International Telecommunication Union. Recommendation X. 1255: *Framework for Discovery of Identity Management Information (Non-Person Entities)*
<http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en>

43 **2 Terminology and Definitions**

44
45 [National Institute of Standards and Technology](#)
46 [Special Publication 800-63-3](#)

47 **Address of Record**

48 The validated and verified location (physical or digital) where an individual can receive
49 communications using approved mechanisms.

51 **Applicant**

52 A subject undergoing the processes of registration and identity proofing.

54 **Assertion**

55 A statement from a verifier to an RP that contains identity information about a subscriber.
56 Assertions may also contain verified attributes.

58 **Assurance**

59 The degree of confidence in the vetting process used to establish the identity of a claimant to
60 whom a credential was, or credentials were, issued, and the degree of confidence that the
61 claimant who uses the credential is the same as the subscriber to whom the credential was
62 issued.

64 **Asymmetric Keys**

65 Two related keys, consisting of a public key and a private key, that are used to perform
66 complementary operations such as encryption and decryption or signature verification and
67 generation.

69 **Attack**

70 An attempt by an unauthorized entity to fool a verifier or an RP into believing that the
71 unauthorized individual in question is the subscriber.

73 **Attacker**

74 A party who acts with malicious intent to compromise a system.

76 **Attribute**

77 A quality or characteristic ascribed to someone or something.

79 **Authentication**

80 Process of determining the validity of one or more credentials used to claim a digital identity.

81
82
83

84 Authentication Protocol

85 A defined sequence of messages between a claimant and a verifier that demonstrates that the
86 claimant has possession and control of one or more valid authenticators to establish their
87 identity, and, optionally, demonstrates that the claimant is communicating with the intended
88 verifier.

89

90 Authenticator

91 Something that the claimant possesses and controls (typically a cryptographic module or
92 password) that is used to authenticate the claimant's identity. In previous editions of SP 800-63,
93 this was referred to as a token.

94

95 Authenticator Assurance Level (AAL)

96 A category describing the authentication process proving that the claimant is in control of a
97 given subscriber's authenticator(s).

98

99 Authenticator Secret

100 The secret value contained within an authenticator.

101

102 Authenticity

103 The property that data originated from their purported source.

104

105 Biometrics

106 Automated recognition of individuals based on their behavioral and biological characteristics.
107 In this document, biometrics may be used to unlock authenticators and prevent repudiation of
108 registration.

109

110 Claimant

111 A subject whose identity is to be verified using one or more authentication protocols.

112

113 Claimed Identity

114 A declaration of unvalidated and unverified personal attributes by the applicant.

115

116 Credential

117 An object or data structure that authoritatively binds an identity, via an identifier or identifiers,
118 and, optionally, additional attributes, to at least one authenticator possessed and controlled by
119 a subscriber. While common usage often assumes that the credential is maintained by the
120 subscriber, this document also uses the term to refer to electronic records maintained by the
121 CSP which establish a binding between the subscriber's authenticator(s) and identity.

122

123 Credential Service Provider (CSP)

124 A trusted entity that issues or registers subscriber authenticators and issues electronic
125 credentials to subscribers. The CSP may encompass Registration Authorities (RAs) and verifiers
126 that it operates. A CSP may be an independent third party, or may issue credentials for its own
127 use.

128 Cryptographic Key

129 A value used to control cryptographic operations, such as decryption, encryption, signature
130 generation or signature verification. For the purposes of this document, key requirements shall
131 meet the minimum requirements stated in Table 2 of NIST SP 800-57 Part 1.

132 See also Asymmetric Keys, Symmetric Key.

133

134 Cryptographic Authenticator

135 An authenticator where the secret is a cryptographic key.

136

137 Digital Authentication

138 The process of establishing confidence in user identities presented digitally to a system. In
139 previous editions of SP 800-63, this was referred to as Electronic Authentication.

140

141 Digital Signature

142 An asymmetric key operation where the private key is used to digitally sign data and the public
143 key is used to verify the signature. Digital signatures provide authenticity protection, integrity
144 protection, and non-repudiation but not confidentiality protection.

145

146 Electronic Authentication (E-Authentication)

147 See Digital Authentication.

148

149 Federal Information Security Management Act (FISMA)

150 Title III of the E-Government Act requiring each federal agency to develop, document, and
151 implement an agency-wide program to provide information security for the information and
152 systems that support the operations and assets of the agency, including those provided or
153 managed by another agency, contractor, or other source.

154

155 Federal Information Processing Standard (FIPS)

156 Under the Information Technology Management Reform Act (Public Law 104-106), the
157 Secretary of Commerce approves standards and guidelines that are developed by the National
158 Institute of Standards and Technology (NIST) for Federal computer systems. These standards
159 and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use
160 government-wide. NIST develops FIPS when there are compelling Federal government
161 requirements such as for security and interoperability and there are no acceptable industry
162 standards or solutions. FIPS documents are available online through the FIPS home page:
163 <http://www.nist.gov/itl/fips>.

164

165 Federation

166 A process that allows for the conveyance of identity and authentication information across a set
167 of networked systems.

168

169 Federation Assurance Level

170 A category describing the assertion protocol utilized by the federation to communicate
171 authentication and attribute information (if applicable) to an RP.

172 **Identity**

173 An attribute or set of attributes that uniquely describe a subject within a given context.

174

175 **Identity Assurance Level (IAL)**

176 A category that conveys the degree of confidence that the applicant's claimed identity is their
177 real identity.

178

179 **Identity Proofing**

180 The process by which a CSP and an RA collect and verify information about a person for the
181 purpose of issuing credentials to that person.

182

183 **Identity Provider (IdP)**

184 The party that manages the subscriber's primary authentication credentials and issues
185 assertions derived from those credentials. This is commonly the CSP as discussed within this
186 document suite.

187

188 **Memorized Secret**

189 A type of authenticator consisting of a character string that is intended to be memorized or
190 memorable by the subscriber, permitting the subscriber to demonstrate something they know
191 as part of an authentication process.

192

193 **Multi-Factor**

194 A characteristic of an authentication system or an authenticator that requires more than one
195 authentication factor for successful authentication. MFA can be performed using a single
196 authenticator that provides more than one factor or by a combination of authenticators that
197 provide different factors. The three authentication factors are something you know, something
198 you have, and something you are.

199

200 **Network**

201 An open communications medium, typically the Internet, that is used to transport messages
202 between the claimant and other parties. Unless otherwise stated, no assumptions are made
203 about the security of the network; it is assumed to be open and subject to active (e.g.,
204 impersonation, man-in-the-middle, session hijacking) and passive (e.g., eavesdropping) attack
205 at any point between the parties (e.g., claimant, verifier, CSP, RP).

206

207 **Password**

208 See memorized secret.

209

210 **Personal Identification Number (PIN)**

211 A memorized secret typically consisting only of decimal digits.

212

213

214 **Personally Identifiable Information (PII)**

215 As defined by OMB Circular [A-130], Personally Identifiable Information means information that
216 can be used to distinguish or trace an individual's identity, either alone or when combined with
217 other information that is linked or linkable to a specific individual.

218

219 **Private Key**

220 The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.

221

222 **Pseudonymous Identifier**

223 A meaningless but unique number that does not allow the RP to infer anything regarding the
224 subscriber but which does permit the RP to associate multiple interactions with the subscriber's
225 claimed identity.

226

227 **Public Key**

228 The public part of an asymmetric key pair that is used to verify signatures or encrypt data.

229

230 **Public Key Certificate**

231 A digital document issued and digitally signed by the private key of a certificate authority that
232 binds an identifier to a subscriber to a public key. The certificate indicates that the subscriber
233 identified in the certificate has sole control and access to the private key. See also [RFC 5280].

234

235 **Public Key Infrastructure (PKI)**

236 A set of policies, processes, server platforms, software and workstations used for the purpose
237 of administering certificates and public-private key pairs, including the ability to issue, maintain,
238 and revoke public key certificates.

239

240 **Registration**

241 The process through which an applicant applies to become a subscriber of a CSP and has their
242 identity validated by the CSP.

243

244 **Relying Party (RP)**

245 An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's
246 assertion of a claimant's identity, typically to process a transaction or grant access to
247 information or a system.

248

249 **Remote**

250 (In the context of remote authentication or remote transaction) An information exchange
251 between network-connected devices where the information cannot be reliably protected end-
252 to-end by a single organization's security controls.

253 Note: Any information exchange across the Internet is considered remote.

254

255 **Risk Assessment**

256 The process of identifying, estimating, and prioritizing risks to organizational operations
257 (including mission, functions, image, or reputation), organizational assets, individuals, and other

258 organizations, resulting from the operation of a system. Part of risk management, incorporates
259 threat and vulnerability analyses, and considers mitigations provided by security controls
260 planned or in place. Synonymous with risk analysis.

261

262 **Risk Management**

263 The program and supporting processes to manage information security risk to organizational
264 operations (including mission, functions, image, reputation), organizational assets, individuals,
265 other organizations, and includes: (i) establishing the context for risk-related activities; (ii)
266 assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

267

268 **Shared Secret**

269 A secret used in authentication that is known to the subscriber and the verifier.

270

271 **Special Publication (SP)**

272 A type of publication issued by NIST. Specifically, the SP 800-series reports on the Information
273 Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its
274 collaborative activities with industry, government, and academic organizations.

275

276 **Subscriber**

277 A party who has received a credential or authenticator from a CSP.

278

279 **Subject**

280 A person, organization, device, hardware, network, software, or service.

281

282 **Symmetric Key**

283 A cryptographic key that is used to perform both the cryptographic operation and its inverse,
284 for example to encrypt and decrypt, or create a message authentication code and to verify the
285 code.

286

287 **Valid**

288 In reference to identity evidence, the quality of not being expired or revoked.

289

290 **Verifier**

291 An entity that verifies the claimant's identity by verifying the claimant's possession and control
292 of one or two authenticators using an authentication protocol. To do this, the verifier may also
293 need to validate credentials that link the authenticator(s) to the subscriber's identifier and
294 check their status.

295

296

297 **Commonwealth of Virginia**
298 **Electronic Identity Management Act**
299 **Chapter 50 of Title 59.1, Code of Virginia¹**

300
301 The following terms shall have the meanings assigned in § 59.1-550, unless the context requires
302 a different meaning:

303
304 **Attribute Provider**

305 An entity, or a supplier, employee, or agent thereof, that acts as the authoritative record of
306 identifying information about an identity credential holder.

307
308 **Commonwealth Identity Management Standards**

309 The minimum specifications and standards that must be included in an identity trust framework
310 so as to define liability pursuant to this chapter that are set forth in guidance documents
311 approved by the Secretary of Technology pursuant to Chapter 4.3 (§ 2.2-436 et seq.) of
312 Title 2.2.

313
314 **Identity Attribute**

315 Identifying information associated with an identity credential holder.

316
317 **Identity Credential**

318 The data, or the physical object upon which the data may reside, that an identity credential
319 holder may present to verify or authenticate his identity in a digital or online transaction.

320
321 **Identity Credential Holder**

322 A person bound to or in possession of an identity credential who has agreed to the terms and
323 conditions of the identity provider.

324
325 **Identity Proofer**

326 A person or entity authorized to act as a representative of an identity provider in the
327 confirmation of a potential identity credential holder's identification and identity attributes
328 prior to issuing an identity credential to a person.

329
330 **Identity Provider**

331 An entity, or a supplier, employee, or agent thereof, certified by an identity trust framework
332 operator to provide identity credentials that may be used by an identity credential holder to
333 assert his identity, or any related attributes, in a digital or online transaction. For purposes of
334 this chapter, "identity provider" includes an attribute provider, an identity proofer, and any
335 suppliers, employees, or agents thereof.

336

¹ The formatting of the definitions in this section has been modified for consistency. The definitions, as formatted in the *Code of Virginia*, may be accessed at <http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/>

337 Identity Trust Framework

338 A digital identity system with established identity, security, privacy, technology, and
339 enforcement rules and policies adhered to by certified identity providers that are members of
340 the identity trust framework. Members of an identity trust framework include identity trust
341 framework operators and identity providers. Relying parties may be, but are not required to be,
342 a member of an identity trust framework in order to accept an identity credential issued by a
343 certified identity provider to verify an identity credential holder's identity.

344

345 Identity Trust Framework Operator

346 The entity that (i) defines rules and policies for member parties to an identity trust framework,
347 (ii) certifies identity providers to be members of and issue identity credentials pursuant to the
348 identity trust framework, and (iii) evaluates participation in the identity trust framework to
349 ensure compliance by members of the identity trust framework with its rules and policies,
350 including the ability to request audits of participants for verification of compliance.

351

352 Relying Party

353 An individual or entity that relies on the validity of an identity credential or an associated
354 trustmark.

355

356 Trustmark

357 A machine-readable official seal, authentication feature, certification, license, or logo that may
358 be provided by an identity trust framework operator to certified identity providers within its
359 identity trust framework to signify that the identity provider complies with the written rules
360 and policies of the identity trust framework.

361

362 **International Telecommunication Union**
363 **Recommendation X. 1255: Framework for Discovery of**
364 **Identity Management Information (Non-Person Entities)**

365
366 **Association**

367 A relationship, if any, between two identified entities.

368
369 **Digital Entity**

370 An entity represented as, or converted to, a machine-independent data structure consisting of
371 one or more elements in digital form that can be parsed by different information systems; the
372 structure helps to enable interoperability among diverse information systems in the Internet.

373
374 **Discovery**

375 The act or process of seeking or locating target information, i.e., obtaining knowledge
376 pertaining to the target.

377
378 **Element**

379 Part of a digital entity consisting of a type-value pair, where the type is represented by a
380 resolvable persistent identifier and the value is the relevant digital information for that type.

381
382 **Federated Registries**

383 A collection of interoperable registries that register metadata and participate in a common set
384 of methods to share information reliably and in a commonly understood format.

385
386 **Identifier**

387 A sequence of bits used to obtain state information about the digital entity being identified;
388 typically, this is done via an appropriate resolution system.

389
390 **Identity Management**

391 A means by which identity management information, whether for a
392 user, a system resource, information or other entities, can be validated.

393
394 **Identity Management Information**

395 Identity-related information including all types of
396 metadata associated with identity, provenance, association and trust.

397
398 **Metadata**

399 Structured information that pertains to the identity of users, systems, services, processes,
400 resources, information or other entities.

401

402

403 Persistent Identifier

404 A unique identifier that resolves to state information about a digital entity and that is
405 resolvable for at least as long as the digital entity exists.

406

407 Provenance

408 Information pertaining to any source of information including the party or
409 parties involved in generating it, introducing it and/or vouching for it.

410

411 Registry

412 A mechanism for registering metadata about digital entities and storing metadata schemas, and
413 which provides an ability to search the registry for persistent identifiers based on the use of the
414 metadata schemas.

415

416 Repository

417 An interface that accepts deposits of digital entities, enables their retention, and provides
418 secure access to the digital entities via their identifiers.

419

420 Resolution System

421 A system that accepts identifiers known to the system as input, and provides relevant state
422 information about the entity being identified.

423

424 Touch Point

425 A registry within a system of federated registries that is selected to interface with a designated
426 registry in another federation, typically for the purposes of peering.

427

428

429 **Additional Terminology and Definitions**430 **Source Cited by Reference in Brackets []**

431

432 **Digital Identity System**433 An Information System that supports Electronic Authentication and the management of a
434 person's Identity in a digital environment. [Referenced in § 59.1-550, Code of Virginia]

435

436 **Information System**437 A discrete set of information resources organized for the collection, processing, maintenance,
438 use, sharing, dissemination, or disposition of information. [NIST Interagency/Internal Report
439 (IR) 7298 r. 2]

440

441 **Participant Requirements**442 A set of rules and policies in an Identity Trust Framework addressing identity, security, privacy,
443 technology, and enforcement, which are assigned to each member type in a Digital Identity
444 System. Member types include Registration Authorities (RAs), Identity Providers (IdPs),
445 Credential Service Providers (CSPs), Verifiers, and Relying Parties (RPs). [Referenced in § 59.1-
446 550, Code of Virginia]

447

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

452

453 **Virtual In-Person Proofing**454 A remote identity person proofing process that employs technical and procedural measures
455 that provide sufficient confidence that the remote session can be considered equivalent to a
456 physical, in-person identity proofing encounter. [NIST SP 800-63A]

457