



1

2 **Identity Assurance Framework:**
3 ***SAC mapping - NIST SP 800-63-2 -***
4 ***(Structured) Electronic Authentication Guidelines***

5 **Version:** 2.0
6 **Date:** 2015-12-17
7 **Status:** Final Report
8 **Approval:** IAWG20151203

9 **Editor:** Richard G. Wilsher
10 Zyigma LLC

11 **Contributors**

12 Members of the Kantara Initiative Identity Assurance Working Group have contributed to
13 review and development of this document.
14

Executive Summary

This mapping was produced as a product of an undertaking sponsored by two Kantara members, to bring the Service Assessment Criteria (KI-IAF 1400) into full alignment with NIST’s SP 800-63-2. It was a specific output of the Statement of Work under which the SAC alignment was performed and is a partial re-structuring of NIST’s SP 800-63-2 with mappings into the SAC v4.0 (as the aligned SAC will be identified), performed under certain self-imposed restrictions (see the following Apologia).

This mapping serves a number of valuable and distinct purposes:

- i) it renders the essential parts of SP 800-63-2 as a much clearer set of requirements than in their original form;
- ii) it provides a reference work which underpins and justifies the revisions made to the SAC v4.0 in order to achieve the alignment;
- iii) it has enabled clarification of parts of the original NIST document which were ambiguous, unclear or otherwise doubtful, and records those clarifications;
- iv) it facilitates service providers wishing to demonstrate their compliance with SP 800-63-2 by providing a set of discretely-referenceable requirements which the original document cannot support;
- v) in addition to the above, it provides clear guidance where a US-specific profile for meeting both Kantara SAC requirements and SP 800-63 compliance should be developed (which would serve the same purpose for any other jurisdiction wishing to adopt SP 800-63);
- vi) by virtue of the two points above, this mapping facilitates both internal and third-party review and assessment of such services;
- vii) finally, this mapping has the potential to act as a future, structurally-improved, revision to SP 800-63, as has been previously discussed with NIST personnel and was an intention of the original tasking.

Readership

This report is intended to be read and used as guidance by:

- a) those designing and implementing Identity and Credential Management Services or components for which they seek Kantara Approval, and who wish to demonstrate their alignment or compliance to NIST SP 800-63-2;
- b) those who wish to develop US-specific profiles of Kantara’s SAC to facilitate the demonstration of strict compliance to SP 800-63-2;
- c) those who are responsible for reviewing or more formally assessing (e.g. as a Kantara-Accredited Assessor) Identity and Credential Management Services against SP 800-63-2.

Feedback

Users of this report are encouraged to provide feedback to Kantara concerning any alternative views on, alternatives to, or enhancement of, the mappings presented herein.

52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92

Apologia

In this mapping Kantara has extended the original text of NIST SP 800-63-2 by inserting sections/headings, paragraph numbering, replacement of some bullet lists by numbered lists, and re-ordering of original content as deemed necessary to facilitate identification of and an equivalence mapping to the actual requirements set forth herein. Edits have been executed for the purposes of re-locating parts of the text for structural and presentational reasons, correcting or clarifying the original text, remedying obvious syntactic or grammatical shortcomings or, more significantly, challenging the reasoning of some few clauses, in which case Kantara’s reasoning for any changes proposed or applied is explained.

The assignment of a new paragraph reference applies only to the single referenced paragraph. If any further paragraphs hold requirements worthy of specific identification they too have been assigned a specific reference.

Un-referenced paragraphs following referenced paragraphs are not intended to be included by or within the preceding reference and are deemed not to hold any worthy statements of requirements.

In undertaking these extensions Kantara has sought not to pervert the original content and meaning of NIST’s source text, and believes it has been successful in that endeavour.

However, so as to protect the innocent, all NIST identification, authority and references to personnel and contributors have been removed or amended to deny its original authority. This document has no authority whatsoever and serves merely as a technical reference for the above-stated purposes.

All Kantara additional text is shown in this font colour and style. No NIST text has been deleted unless:

- i) it has been re-positioned to enable the re-structuring or cross-referencing; or*
- ii) it has been amended to suit its modified context.*

Such revisions are indicated using ‘track change’-type format, i.e. deleted is red-lined through, inserted is green.

Where paragraph clause references / indexes have been added these have been committed with the primary objective of enabling the mappings and the adoption of a consistent format of indexing at sub-clause and sub-sub-clause levels. It is recognized that in so doing inconsistencies and non-standard practices may have been introduced, but the task has not been to provide an internally-consistent structure (given the starting point) nor a proof-read revision of SP 800-63-2, and so the reader is requested to accept the document as is.

Additionally, an attempt has been made to clarify and justify the restructuring regarding the Assurance Level at which particular clauses (requirements) apply. This has been accomplished by pre-fixing sections and sometimes discrete paragraphs with italicized text stating the applicable Assurance Level or Levels.

Finally, some requirements have been added in green text, where discussion with the original Editor-in-Chief has confirmed this to have been the intention.

We trust that no NIST personnel were harmed or traumatized by the execution of this work.

*The mapping has been conducted specifically against the following clauses:
§5.3, §6.3, §7.3, §8.3, §9.3.2.*

93
94

Table of Contents

95	1. Purpose.....	2
96	2. Introduction.....	2
97	3. Definitions and Abbreviations	6
98	4. E-Authentication Model.....	15
99	4.1. Overview	15
100	4.2. Subscribers, Registration Authorities and Credential Service Providers.....	18
101	4.3. Tokens.....	18
102	4.4. Credentials	20
103	4.5. Authentication Process.....	21
104	4.6. Assertions.....	21
105	4.7. Relying Parties	22
106	4.8. Calculating the Overall Authentication Assurance Level.....	22
107	5. Registration and Issuance Processes	24
108	5.1. Overview	24
109	5.2. Registration and Issuance Threats	25
110	5.2.1. Overview	25
111	5.2.2. Threat Mitigation Strategies	25
112	5.3. Registration and Issuance Assurance Levels	28
113	5.3.1. General Requirements per Assurance Level.....	28
114	5.3.2. Requirements for Educational and Financial Institutions, and other Organizations	39
115	5.3.3. Requirements for Certificates Issued under FPKI and Mapped Policies.....	41
116	5.3.4. Requirements for One-Time Use	41
117	5.3.5. Requirements for Derived Credentials.....	42
118	6. Tokens.....	44
119	6.1. Overview	44
120	6.1.1. Single-factor versus Multi-factor Tokens	45
121	6.1.2. Token Types.....	45
122	6.1.3. Token Usage	47
123	6.1.4. Multi-Stage Authentication Using Tokens	47
124	6.1.5. Assurance Level Escalation	47
125	6.2. Token Threats	48
126	6.2.1. Threat Mitigation Strategies	49
127	6.3. Token Assurance Levels	50
128	6.3.1. Requirements per Assurance Level	50
129	7. Token and Credential Management	57
130	7.1. Overview	57
131	7.1.1. Categorizing Credentials.....	57
132	7.1.2. Token and Credential Management Activities	57
133	7.2. Token and Credential Management Threats	59
134	7.2.1. Threat Mitigation Strategies	61
135	7.3. Token and Credential Management Assurance Levels.....	61
136	7.3.1. Requirements per Assurance Level	61
137	7.3.2. Relationship of PKI Policies to E-Authentication Assurance Levels	69
138	8. Authentication Process.....	70
139	8.1. Overview	70
140	8.2. Authentication Process Threats.....	71

141	8.2.1.	Other Threats	72
142	8.2.2.	Threat Mitigation Strategies	73
143	8.2.3.	Throttling Mechanisms	75
144	8.2.4.	Phishing and Pharming (Verifier Impersonation): Supplementary Countermeasures.....	76
145	8.3.	Authentication Process Assurance Levels	79
146	8.3.1.	Threat Resistance per Assurance Level	79
147		[KI-IAF: See details below].....	79
148	8.3.2.	Requirements per Assurance Level	79
149	9.	Assertions.....	83
150	9.1.	Overview	83
151	9.1.1.	Cookies	86
152	9.1.2.	Security Assertion Markup Language (SAML) Assertions.....	87
153	9.1.3.	Kerberos Tickets	87
154	9.2.	Assertion Threats	88
155	9.2.1.	Threat Mitigation Strategies	90
156	9.3.	Assertion Assurance Levels	92
157	9.3.1.	Threat Resistance per Assurance Level	92
158	9.3.2.	Requirements per Assurance Level	92
159	10.	References.....	101
160	10.1.	General References	101
161	10.2.	NIST Special Publications	102
162	10.3.	Federal Information Processing Standards	103
163	10.4.	Certificate Policies	103
164	Appendix A: Estimating Entropy and Strength		103
165	Password Entropy		103
166	A.1	Randomly Selected Passwords	105
167	A.2	User Selected Passwords.....	105
168	A.3	Other Types of Passwords	108
169	Appendix B: Mapping of Federal PKI Certificate Policies to E-authentication Assurance Levels		110
171			
170			

172

173 1. Purpose

174

175 This recommendation provides technical guidelines to agencies for the implementation of electronic
176 authentication (e-authentication).

177 2. Introduction

178

179 Electronic authentication (e-authentication) is the process of establishing confidence in user identities
180 electronically presented to an information system. E-authentication presents a technical challenge when this
181 process involves the remote authentication of individual people over a network. This recommendation
182 provides technical guidelines to agencies to allow an individual person to remotely authenticate his/her
183 identity to a Federal Information Technology (IT) system. This recommendation also provides guidelines for
184 Registration Authorities (RAs), Verifiers, Relying Parties (RPs) and Credential Service Providers (CSPs).

185 Current government systems do not separate the functions of authentication and attribute providers. In some
186 applications, these functions are provided by different parties. While a combined authentication and attribute
187 provider model is used in this document, it does not preclude agencies from separating these functions.

188 These technical guidelines supplement OMB guidance, *E-Authentication Guidance for Federal Agencies*
189 [[OMB M-04-04](#)] and supersede NIST SP 800-63. OMB M-04-04 defines four levels of assurance, Levels 1
190 to 4, in terms of the consequences of authentication errors and misuse of credentials. Level 1 is the lowest
191 assurance level and Level 4 is the highest. The guidance defines the required level of authentication
192 assurance in terms of the likely consequences of an authentication error. As the consequences of an
193 authentication error become more serious, the required level of assurance increases. The OMB guidance
194 provides agencies with criteria for determining the level of e-authentication assurance required for specific
195 electronic transactions and systems, based on the risks and their likelihood of occurrence.

196 OMB guidance outlines a 5 step process by which agencies should meet their e-authentication assurance
197 requirements:

198

- 199 1. *Conduct a risk assessment of the government system* – No specific risk assessment methodology is
200 prescribed for this purpose, however the e-RA tool¹ at <http://www.idmanagement.gov/> is an
201 example of a suitable tool and methodology, while NIST Special Publication (SP) 800-30 [[SP](#)
202 [800-30](#)] offers a general process for Risk Assessment and Risk Mitigation.
- 203 2. *Map identified risks to the appropriate assurance level* – Section 2.2 of OMB M-04-04 provides
204 the guidance necessary for agencies to perform this mapping.
- 205 3. *Select technology based on e-authentication technical guidance* – After the appropriate assurance
206 level has been determined, OMB guidance states that agencies should select technologies that
207 meet the corresponding technical requirements, as specified by this document. Some agencies
208 may possess existing e-authentication technology. Agencies should verify that any existing
209 technology meets the requirements specified in this document.

¹ At the time of publication, the specific URL for this tool is at <http://www.idmanagement.gov/drilldown.cfm?action=era>.
Alternatively, the tool can be found by searching for “Electronic Risk and Requirements Assessment (e-RA)” at
<http://www.idmanagement.gov/>.

- 210 4. *Validate that the implemented system has met the required assurance level* – As some
211 implementations may create or compound particular risks, agencies should conduct a final
212 validation to confirm that the system achieves the required assurance level for the user-to-agency
213 process. NIST SP 800-53A [[SP 800-53A](#)] provides guidelines for the assessment of the
214 implemented system during the validation process. Validation should be performed as part of a
215 security authorization process as described in NIST SP 800-37, Revision 1 [[SP 800-37](#)].
- 216 5. *Periodically reassess the information system to determine technology refresh requirements* – The
217 agency shall periodically reassess the information system to ensure that the identity authentication
218 requirements continue to be satisfied. NIST SP 800-37, Revision 1 [[SP 800-37](#)] provides
219 guidelines on the frequency, depth and breadth of periodic reassessments. As with the initial
220 validation process, agencies should follow the assessment guidelines specified in SP 800-53A [[SP](#)
221 [800-53A](#)] for conducting the security assessment.

222 This document provides guidelines for implementing the third step of the above process. In particular, this
223 document states specific technical requirements for each of the four levels of assurance in the following
224 areas:

- 225 a) Registration and identity proofing of Applicants (covered in Section 5);
- 226 b) Tokens (typically a cryptographic key or password) for authentication (covered in Section 6);
- 227 c) Token and credential management mechanisms used to establish and maintain token and
228 credential information (covered in Section 7);
- 229 d) Protocols used to support the authentication mechanism between the Claimant and the Verifier
230 (covered in Section 8);
- 231 e) Assertion mechanisms used to communicate the results of a remote authentication, if these results
232 are sent to other parties (covered in Section 9).

233 The overall authentication assurance level is determined by the lowest assurance level achieved in any of the
234 areas listed above.

235 Agencies may adjust the level of assurance using additional risk mitigation measures. Easing credential
236 assurance level requirements may increase the size of the enabled customer pool, but agencies shall ensure
237 that this does not corrupt the system’s choice of the appropriate assurance level. Alternatively, agencies may
238 consider partitioning the functionality of an e-authentication enabled application to allow less sensitive
239 functions to be available at a lower level of authentication and attribute assurance, while more sensitive
240 functions are available only at a higher level of assurance.

241 These technical guidelines cover remote electronic authentication of human users to IT systems over a
242 network. They do not address the authentication of a person who is physically present, for example, for
243 access to buildings, although some credentials and tokens that are used remotely may also be used for local
244 authentication. These technical guidelines establish requirements that Federal IT systems and service
245 providers participating in authentication protocols be authenticated to Subscribers. However, these guidelines
246 do not specifically address machine-to-machine (such as router-to-router) authentication, or establish specific
247 requirements for issuing authentication credentials and tokens to machines and servers when they are used in
248 e-authentication protocols with people.

249 The paradigm of this document is that individuals are enrolled and undergo a registration process in which
250 their identity is bound to a token. Thereafter, the individuals are remotely authenticated to systems and
251 applications over a network, using the token in an authentication protocol. The authentication protocol allows

252 an individual to demonstrate to a Verifier that he or she has possession and control of the token², in a manner
253 that protects the token secret from compromise by different kinds of attacks. Higher authentication assurance
254 levels require use of stronger tokens, better protection of the token and related secrets from attacks, and
255 stronger registration procedures.

256 This document focuses on tokens that are difficult to forge because they contain some type of secret
257 information that is not available to unauthorized parties and that is preferably not used in unrelated contexts.
258 Certain authentication technologies, particularly biometrics and knowledge based authentication, use
259 information that is private rather than secret. While they are discussed to a limited degree, they are largely
260 avoided because their security is often weak or difficult to quantify³, especially in the remote situations that
261 are the primary scope of this document.

262 Knowledge based authentication achieves authentication by testing the personal knowledge of the individual
263 against information obtained from public databases. As this information is considered private but not actually
264 secret, confidence in the identity of an individual can be hard to achieve. In addition, the complexity and
265 interdependencies of knowledge based authentication systems are difficult to quantify. However, knowledge
266 based authentication techniques are included as part of registration in this document. In addition, pre-
267 registered knowledge techniques are accepted as an alternative to passwords at lower levels of assurance.

268 Biometric characteristics do not constitute secrets suitable for use in the conventional remote authentication
269 protocols addressed in this document either. In the local authentication case, where the Claimant is observed
270 by an attendant and uses a capture device controlled by the Verifier, authentication does not require that
271 biometrics be kept secret. This document supports the use of biometrics to “unlock” conventional
272 authentication tokens, to prevent repudiation of registration, and to verify that the same individual
273 participates in all phases of the registration process.

274 This document identifies minimum technical requirements for remotely authenticating identity. Agencies
275 may determine based on their risk analysis that additional measures are appropriate in certain contexts. In
276 particular, privacy requirements and legal risks may lead agencies to determine that additional authentication
277 measures or other process safeguards are appropriate. When developing e-authentication processes and
278 systems, agencies should consult *OMB Guidance for Implementing the Privacy Provisions of the E-
279 Government Act of 2002* [[OMB M-03-22](#)]. See the *Guide to Federal Agencies on Implementing Electronic
280 Processes* [[DOJ 2000](#)] for additional information on legal risks, especially those that are related to the need to
281 satisfy legal standards of proof and prevent repudiation, as well as *Use of Electronic Signatures in Federal
282 Organization Transactions* [[GSA ESIG](#)].

283 Additionally, Federal agencies implementing these guidelines should adhere to the requirements of Title III
284 of the E-Government Act, entitled the *Federal Information Security Management Act* [[FISMA](#)], and the
285 related NIST standards and guidelines. FISMA directs Federal agencies to develop, document, and
286 implement agency-wide programs to provide information security for the information and information
287 systems that support the operations and assets of the agency. This includes the security authorization of IT
288 systems that support e-authentication. It is recommended that non-Federal entities implementing these
289 guidelines follow equivalent standards of security management, certification and accreditation to ensure the
290 secure operations of their e-authentication systems.

² See Section 3 for the definition of “token” as used in this document, which is consistent with the original version of SP 800-63, but there are a variety of definitions used in the area of authentication.

³ For example, see article by V. Griffith and M. Jakobsson, entitled “Messin’ with Texas – Deriving Mother’s Maiden Names Using Public Records,” in *RSA CryptoBytes*, Winter 2007.

291 This document has been updated to reflect current (token) technologies and has been restructured to provide a
292 better understanding of the e-authentication architectural model used here. Additional (minimum) technical
293 requirements have been specified for the CSP, protocols utilized to transport authentication information, and
294 assertions if implemented within the e-authentication model. Other changes since NIST SP 800-63 was
295 originally published include:

- 296 f) Recognition of more types of tokens, including pre-registered knowledge token, look-up secret token,
297 out-of-band token, as well as some terminology changes for more conventional token types;
- 298 g) Detailed requirements for assertion protocols and Kerberos;
- 299 h) A new section on token and credential management;
- 300 i) Simplification of guidelines for password entropy and throttling;
- 301 j) Emphasis that the document is aimed at Federal IT systems;
- 302 k) Recognition of different models, including a broader e-authentication model (in contrast to the
303 simpler model common among Federal IT systems shown in Figure 1) and an additional assertion
304 model, the Proxy Model, presented in Figure 6;
- 305 l) Clarification of differences between Levels 3 and 4 in Table 12; and
- 306 m) New guidelines that permit leveraging existing credentials to issue derived credentials.

307
308 The subsequent sections present a series of recommendations for the secure implementation of RAs, CSPs,
309 Verifiers, and RPs. It should be noted that secure implementation of any one of these can only provide the
310 desired level of assurance if the others are also implemented securely. Therefore, the following assumptions
311 have been made in this guideline:

- 312 n) RAs, CSPs, and Verifiers are trusted entities. Agencies implementing any of the above trusted
313 entities have some assurance that all other trusted entities with which the agency interacts are also
314 implemented appropriately for the desired security level.
- 315 o) The RP is not considered a trusted entity. However, in some authentication systems the Verifier
316 maintains a relationship with the RP to facilitate secure communications and may employ security
317 controls which only attain their full value when the RP acts responsibly. The Subscriber also trusts the
318 RP to properly perform the requested service and to follow all relevant privacy policy.
- 319 p) It is assumed that there exists a process of certification through which agencies can obtain the above
320 assurance for trusted entities which they do not implement themselves.
- 321 q) A trusted entity is considered to be implemented appropriately if it complies with the
322 recommendations in this document and does not behave maliciously.
- 323 r) While it is generally assumed that trusted entities will not behave maliciously, this document does
324 contain some recommendations to reduce and isolate any damage done by a malicious or negligent
325 trusted entity.

326

327
 328
 329
 330
 331

3. Definitions and Abbreviations

There are a variety of definitions used in the area of authentication. We have kept terms consistent with the original version of SP 800-63. Pay careful attention to how the terms are defined here.

Active Attack	An attack on the authentication protocol where the Attacker transmits data to the Claimant, Credential Service Provider, Verifier, or Relying Party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking.
Address of Record	The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.
Approved	Federal Information Processing Standard (FIPS) approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.
Applicant	A party undergoing the processes of registration and identity proofing.
Assertion	A statement from a Verifier to a Relying Party (RP) that contains identity information about a Subscriber. Assertions may also contain verified attributes.
Assertion Reference	A data object, created in conjunction with an assertion, which identifies the Verifier and includes a pointer to the full assertion held by the Verifier.
Assurance	In the context of OMB M-04-04 and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
Asymmetric Keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Attack	An attempt by an unauthorized individual to fool a Verifier or a Relying Party into believing that the unauthorized individual in question is the Subscriber.
Attacker	A party who acts with malicious intent to compromise an information system.
Attribute	A claim of a named quality or characteristic inherent in or ascribed to someone or something. (See term in [ICAM] for more information.)
Authentication	The process of establishing confidence in the identity of users or information systems.
Authentication Protocol	A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier.
Authentication Protocol Run	An exchange of messages between a Claimant and a Verifier that results in authentication (or authentication failure) between the two parties.

Authentication Secret	<p>A generic term for any secret value that could be used by an Attacker to impersonate the Subscriber in an authentication protocol.</p> <p>These are further divided into <i>short-term authentication secrets</i>, which are only useful to an Attacker for a limited period of time, and <i>long-term authentication secrets</i>, which allow an Attacker to impersonate the Subscriber until they are manually reset. The token secret is the canonical example of a long term authentication secret, while the token authenticator, if it is different from the token secret, is usually a short term authentication secret.</p>
Authenticity	The property that data originated from its purported source.
Bearer Assertion	An assertion that does not provide a mechanism for the Subscriber to prove that he or she is the rightful owner of the assertion. The RP has to assume that the assertion was issued to the Subscriber who presents the assertion or the corresponding assertion reference to the RP.
Bit	A binary digit: 0 or 1.
Biometrics	<p>Automated recognition of individuals based on their behavioral and biological characteristics.</p> <p>In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration.</p>
Certificate Authority (CA)	A trusted entity that issues and revokes public key certificates.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certificate Authority. See [RFC 5280] .
Challenge-Response Protocol	An authentication protocol where the Verifier sends the Claimant a challenge (usually a random value or a nonce) that the Claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the Verifier. The Verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret.
Claimant	A party whose identity is to be verified using an authentication protocol.
Claimed Address	<p>The physical location asserted by an individual (e.g. an applicant) where he/she can be reached. It includes the residential street address of an individual and may also include the mailing address of the individual.</p> <p>For example, a person with a foreign passport, living in the U.S., will need to give an address when going through the identity proofing process. This address would not be an “address of record” but a “claimed address.”</p>
Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)	An interactive feature added to web-forms to distinguish use of the form by humans as opposed to automated agents. Typically, it requires entering text corresponding to a distorted image or from a sound stream.

Cookie	<p>A character string, placed in a web browser’s memory, which is available to websites within the same Internet domain as the server that placed them in the web browser.</p> <p>Cookies are used for many purposes and may be assertions or may contain pointers to assertions. See Section 9.1.1 for more information.</p>
Credential	<p>An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.</p> <p>While common usage often assumes that the credential is maintained by the Subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the Subscriber’s token and identity.</p>
Credential Service Provider (CSP)	<p>A trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and Verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.</p>
Cross Site Request Forgery (CSRF)	<p>An attack in which a Subscriber who is currently authenticated to an RP and connected through a secure session, browses to an Attacker’s website which causes the Subscriber to unknowingly invoke unwanted actions at the RP.</p> <p>For example, if a bank website is vulnerable to a CSRF attack, it may be possible for a Subscriber to unintentionally authorize a large money transfer, merely by viewing a malicious link in a webmail message while a connection to the bank is open in another browser window.</p>
Cross Site Scripting (XSS)	<p>A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable.</p>
Cryptographic Key	<p>A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57 Part 1.</p> <p>See also Asymmetric keys, Symmetric key.</p>
Cryptographic Token	<p>A token where the secret is a cryptographic key.</p>
Data Integrity	<p>The property that data has not been altered by an unauthorized entity.</p>
Derived Credential	<p>A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process.</p>
Digital Signature	<p>An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation.</p>
Eavesdropping Attack	<p>An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant.</p>

Electronic Authentication (E-Authentication)	The process of establishing confidence in user identities electronically presented to an information system.
Entropy	A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits. See Appendix A .
Extensible Mark-up Language (XML)	Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them.
Federal Bridge Certification Authority (FBCA)	The FBCA is the entity operated by the Federal Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs.
Federal Information Security Management Act (FISMA)	Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
Federal Information Processing Standard (FIPS)	Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. See background information for more details. FIPS documents are available online through the FIPS home page: http://www.nist.gov/itl/fips.cfm
Guessing Entropy	A measure of the difficulty that an Attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an Attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The Attacker is assumed to know the actual password frequency distribution. See Appendix A .
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and 2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
Holder-of-Key Assertion	An assertion that contains a reference to a symmetric key or a public key (corresponding to a private key) held by the Subscriber. The RP may authenticate the Subscriber by verifying that he or she can indeed prove possession and control of the referenced key.
Identity	A set of attributes that uniquely describe a person within a given context.
Identity Proofing	The process by which a CSP and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person.

Kerberos	<p>A widely used authentication protocol developed at MIT. In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob.</p> <p>When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to- KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users.</p>
Knowledge Based Authentication	<p>Authentication of an individual based on knowledge of information associated with his or her claimed identity in public databases. Knowledge of such information is considered to be private rather than secret, because it may be used in contexts other than authentication to a Verifier, thereby reducing the overall assurance associated with the authentication process.</p>
Man-in-the-Middle Attack (MitM)	<p>An attack on the authentication protocol run in which the Attacker positions himself or herself in between the Claimant and Verifier so that he can intercept and alter data traveling between them.</p>
Message Authentication Code (MAC)	<p>A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection.</p>
Min-entropy	<p>A measure of the difficulty that an Attacker has to guess the most commonly chosen password used in a system. In this document, entropy is stated in bits. When a password has n-bits of min-entropy then an Attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The Attacker is assumed to know the most commonly used password(s). See Appendix A.</p>
Multi-Factor	<p>A characteristic of an authentication system or a token that uses more than one authentication factor.</p> <p>The three types of authentication factors are something you know, something you have, and something you are.</p>
Network	<p>An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at any point between the parties (e.g., Claimant, Verifier, CSP or RP).</p>
Nonce	<p>A value used in security protocols that is never repeated with the same key. For example, nonces used as challenges in challenge-response authentication protocols must not be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.</p>
Off-line Attack	<p>An attack where the Attacker obtains some data (typically by eavesdropping on an authentication protocol run or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.</p>

Online Attack	An attack against an authentication protocol where the Attacker either assumes the role of a Claimant with a genuine Verifier or actively alters the authentication channel.
Online Guessing Attack	An attack in which an Attacker performs repeated logon trials by guessing possible values of the token authenticator.
Passive Attack	An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping).
Password	A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.
Personal Identification Number (PIN)	A password consisting only of decimal digits.
Personal Identity Verification (PIV) Card	Defined by [FIPS 201] as a physical artifact (e.g., identity card, smart card) issued to federal employees and contractors that contains stored credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
Personally Identifiable Information (PII)	Defined by GAO Report 08-536 as “Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”
Pharming	An attack in which an Attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the Subscriber to be misdirected to a forged Verifier/RP, which could cause the Subscriber to reveal sensitive information, download harmful software or contribute to a fraudulent act.
Phishing	An attack in which the Subscriber is lured (usually through an email) to interact with a counterfeit Verifier/RP and tricked into revealing information that can be used to masquerade as that Subscriber to the real Verifier/RP.
Possession and control of a token	The ability to activate and use the token in an authentication protocol.
Practice Statement	A formal statement of the practices followed by the parties to an authentication process (i.e., RA, CSP, or Verifier). It usually describes the policies and practices of the parties and can become legally binding.
Private Credentials	Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the token. (For more discussion, see Section 7.1.1.)
Private Key	The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.
Protected Session	A session wherein messages between two participants are encrypted and integrity is protected using a set of shared secrets called session keys. A participant is said to be <i>authenticated</i> if, during the session, he, she or it proves possession of a long term token in addition to the session keys, and if the other party can verify the identity associated with that token. If both participants are authenticated, the protected session is said to be <i>mutually authenticated</i> .

Pseudonym	A false name. In this document, all unverified names are assumed to be pseudonyms.
Public Credentials	Credentials that describe the binding in a way that does not compromise the token. (For more discussion, see Section 7.1.1.)
Public Key	The public part of an asymmetric key pair that is used to verify signatures or encrypt data.
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certificate authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber identified in the certificate has sole control and access to the private key. See also [RFC 5280].
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration	The process through which an Applicant applies to become a Subscriber of a CSP and an RA validates the identity of the Applicant on behalf of the CSP.
Registration Authority (RA)	A trusted entity that establishes and vouches for the identity or attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Relying Party (RP)	An entity that relies upon the Subscriber's token and credentials or a Verifier's assertion of a Claimant's identity, typically to process a transaction or grant access to information or a system.
Remote	<i>(As in remote authentication or remote transaction)</i> An information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. Note: Any information exchange across the Internet is considered remote.
Replay Attack	An attack in which the Attacker is able to replay previously captured messages (between a legitimate Claimant and a Verifier) to masquerade as that Claimant to the Verifier or vice versa.
Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.
Salt	A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an Attacker.
Secondary Authenticator	A temporary secret, issued by the Verifier to a successfully authenticated Subscriber as part of an assertion protocol. This secret is subsequently used, by the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer assertions, assertion references, and Kerberos session keys.
Secure Sockets Layer (SSL)	An authentication and security protocol widely implemented in browsers and web servers. SSL has been superseded by the newer Transport Layer Security (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.

Security Assertion Mark-up Language (SAML)	An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. See [SAML].
SAML Authentication Assertion	A SAML assertion that conveys information from a Verifier to an RP about a successful act of authentication that took place between the Verifier and a Subscriber.
Session Hijack Attack	An attack in which the Attacker is able to insert himself or herself between a Claimant and a Verifier subsequent to a successful authentication exchange between the latter two parties. The Attacker is able to pose as a Subscriber to the Verifier or vice versa to control session data exchange. Sessions between the Claimant and the Relying Party can also be similarly compromised.
Shared Secret	A secret used in authentication that is known to the Claimant and the Verifier.
Social Engineering	The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust.
Special Publication (SP)	A type of publication issued by NIST. Specifically, the Special Publication 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.
Strongly Bound Credentials	Credentials that describe the binding between a user and token in a tamper-evident fashion. (For more discussion, see Section 7.1.1.)
Subscriber	<p>A party who has received a credential or token from a CSP. <i>[KI-IAF: Kantara follows the model of ISO/IEC 29115 and ETSI TS 101 456, TS 102 042 & TS 102 158 in distinguishing between Subscriber and Subject in the following way:</i></p> <p>Subscriber: A party that has entered into an agreement to use an electronic trust service. A Subscriber and a Subject can be the same entity.</p> <p>Subject: An entity that is able to use an electronic trust service subject to agreement with an associated Subscriber. A Subject and a Subscriber can be the same entity.</p> <p><i>No attempt has been made to make any differentiation in the original NIST text which, by definition, effectively assumes the Kantara definition for ‘Subject’, but users of this alignment should be aware of the different implications of ‘Subscriber’ in each domain. It is assumed that the Kantara phrase “able to use a ... service” implies that they have received a credential or token from the CSP providing the electronic trust service.]</i></p>
Symmetric Key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.
Token	Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant’s identity.
Token Authenticator	The output value generated by a token. The ability to generate valid token authenticators on demand proves that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependent upon the token authenticator, but they may or may not explicitly contain it.

Token Secret	The secret value, contained within a token, which is used to derive token authenticators.
Transport Layer Security (TLS)	An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 2246] , [RFC 3546] , and [RFC 5246] . TLS is similar to the older Secure Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52, <i>Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations</i> specifies how TLS is to be used in government applications.
Trust Anchor	A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate).
Unverified Name	A Subscriber name that is not verified as meaningful by identity proofing.
Valid	In reference to an ID, the quality of not being expired or revoked.
Verified Name	A Subscriber name that has been verified by identity proofing.
Verifier	An entity that verifies the Claimant’s identity by verifying the Claimant’s possession and control of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status.
Verifier Impersonation Attack	A scenario where the Attacker impersonates the Verifier in an authentication protocol, usually to capture information that can be used to masquerade as a Claimant to the real Verifier.
Weakly Bound Credentials	Credentials that describe the binding between a user and token in a manner than can be modified without invalidating the credential. (For more discussion, see Section 7.1.1.)
Zeroize	Overwrite a memory location with data consisting entirely of bits with the value zero so that the data is destroyed and not recoverable. This is often contrasted with deletion methods that merely destroy reference to data within a file system rather than the data itself.
Zero-knowledge Password Protocol	A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the Verifier. Examples of such protocols are EKE, SPEKE and SRP.

332

333

334 4. E-Authentication Model

335 [KI-IAF: No mapping is undertaken in this section, which is considered to be discursive.]

336 4.1. Overview

337 In accordance with [OMB M-04-04], e-authentication is the process of establishing confidence in user
338 identities electronically presented to an information system. Systems can use the authenticated identity to
339 determine if that individual is authorized to perform an electronic transaction. In most cases, the
340 authentication and transaction take place across an open network such as the Internet; however, in some cases
341 access to the network may be limited and access control decisions may take this into account.

342 The e-authentication model used in these guidelines reflects current technologies and architectures used in
343 government. More complex models that separate functions, such as issuing credentials and providing
344 attributes, among larger numbers of parties are also possible and may have advantages in some classes of
345 applications. While a simpler model is used in this document, it does not preclude agencies from separating
346 these functions.

347 E-authentication begins with *registration*. The usual sequence for registration proceeds as follows. An
348 *Applicant* applies to a *Registration Authority (RA)* to become a *Subscriber* of a *Credential Service Provider*
349 (*CSP*). If approved, the Subscriber is issued a *credential* by the CSP which binds a *token* to an identifier (and
350 possibly one or more attributes that the RA has verified). The token may be issued by the CSP, generated
351 directly by the Subscriber, or provided by a third party. The CSP registers the token by creating a *credential*
352 that binds the token to an identifier and possibly other attributes that the RA has verified. The token and
353 credential may be used in subsequent authentication events.

354 The name specified in a credential may either be a *verified name* or an *unverified name*. If the RA has
355 determined that the name is officially associated with a real person and the Subscriber is the person who is
356 entitled to use that identity, the name is considered a verified name. If the RA has not verified the
357 Subscriber's name, or the name is known to differ from the official name, the name is considered a
358 *pseudonym*. The process used to verify a Subscriber's association with a name is called identity proofing,
359 and is performed by an RA that registers Subscribers with the CSP. At Level 1, identity proofing is not
360 required so names in credentials and assertions are assumed to be pseudonyms. At Level 2, identity proofing
361 is required, but the credential may assert the verified name or a pseudonym. In the case of a pseudonym, the
362 CSP shall retain the name verified during registration. Level 2 credentials and assertions shall specify
363 whether the name is a verified name or a pseudonym. This information assists *Relying Parties (RPs)* in
364 making access control or authorization decisions. In most cases, only verified names may be specified in
365 credentials and assertions at Levels 3 and 4.⁴ (The required use of a verified name at higher levels of
366 assurance is derived from OMB M-04-04 and is specific to Federal IT systems, rather than a general e-
367 authentication requirement.)

368 In this document, the party to be authenticated is called a *Claimant* and the party verifying that identity is
369 called a *Verifier*. When a *Claimant* successfully demonstrates possession and control of a token to a *Verifier*
370 through an *authentication protocol*, the Verifier can verify that the Claimant is the Subscriber named in the
371 corresponding credential. The Verifier passes on an assertion about the identity of the Subscriber to the

⁴ Note that [FIPS 201] permits authorized pseudonyms in limited cases and does not differentiate between credentials using authorized pseudonyms. Nothing in these guidelines should be interpreted as contravening the contents of the FIPS or constraining the use of these authorized pseudonymous credentials. See Appendix B for the level of PIV credentials.

372 Relying Party (RP). That assertion includes identity information about a Subscriber, such as the Subscriber
373 name, an identifier assigned at registration, or other Subscriber attributes that were verified in the registration
374 process (subject to the policies of the CSP and the needs of the application). Where the Verifier is also the
375 RP, the assertion may be implicit. The RP can use the authenticated information provided by the Verifier to
376 make access control or authorization decisions.

377 Authentication establishes confidence in the Claimant's identity, and in some cases in the Claimant's
378 personal attributes (for example the Subscriber is a US Citizen, is a student at a particular university, or is
379 assigned a particular number or code by an agency or organization). Authentication does not determine the
380 Claimant's authorizations or access privileges; this is a separate decision. RPs (e.g., government agencies)
381 will use a Subscriber's authenticated identity and attributes with other factors to make access control or
382 authorization decisions.

383 As part of authentication, mechanisms such as device identity or geo-location could be used to identify or
384 prevent possible authentication false positives. While these mechanisms do not directly increase the
385 assurance level for authentication, they can enforce security policies and mitigate risks. In many cases, the
386 authentication process and services will be shared by many applications and agencies. However, it is the
387 individual agency or application acting as the RP that shall make the decision to grant access or process a
388 transaction based on the specific application requirements.

389 The various entities and interactions that comprise the e-authentication model used here are illustrated below
390 in Figure 1. The shaded box on the left shows the registration, credential issuance, maintenance activities,
391 and the interactions between the Subscriber/Claimant, the RA and the CSP. The usual sequence of
392 interactions is as follows:

- 393 1. An individual Applicant applies to an RA through a registration process.
- 394 2. The RA identity proofs that Applicant.
- 395 3. On successful identity proofing, the RA sends the CSP a registration confirmation message.
- 396 4. A secret token and a corresponding credential are established between the CSP and the new
397 Subscriber.
- 398 5. The CSP maintains the credential, its status, and the registration data collected for the lifetime of
399 the credential (at a minimum).⁵ The Subscriber maintains his or her token.

400 Other sequences are less common, but could also achieve the same functional requirements.

401 The shaded box on the right side of Figure 1 shows the entities and the interactions related to using a token
402 and credential to perform e-authentication. When the Subscriber needs to authenticate to perform a
403 transaction, he or she becomes a Claimant to a Verifier. The interactions are as follows:

- 404 1. The Claimant proves to the Verifier that he or she possesses and controls the token through an
405 authentication protocol.
- 406 2. The Verifier interacts with the CSP to validate the credential that binds the Subscriber's identity
407 to his or her token.

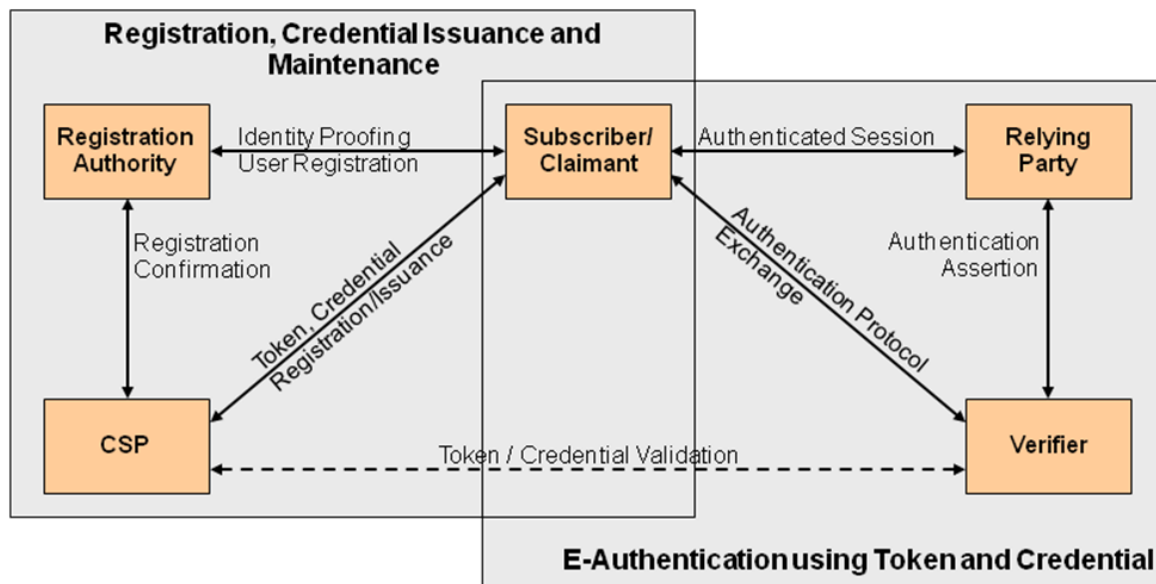
⁵ CSPs may be required to maintain this information beyond the lifetime of the credential to support auditing or satisfy archiving requirements.

- 408 3. If the Verifier is separate from the RP (application), the Verifier provides⁶ an assertion about the
 409 Subscriber to the RP, which uses the information in the assertion to make an access control or
 410 authorization decision.
- 411 4. An authenticated session is established between the Subscriber and the RP.

412 In some cases the Verifier does not need to directly communicate with the CSP to complete the
 413 authentication activity (e.g., some uses of digital certificates). Therefore, the dashed line between the Verifier
 414 and the CSP represents a logical link between the two entities rather than a physical link. In some
 415 implementations, the Verifier, RP and the CSP functions may be distributed and separated as shown in Figure
 416 1; however, if these functions reside on the same platform, the interactions between the components are local
 417 messages between applications running on the same system rather than protocols over shared untrusted
 418 networks.

419 As noted above, CSPs maintain status information about credentials they issue. CSPs will generally assign a
 420 finite lifetime when issuing credentials to limit the maintenance period. When the status changes, or when
 421 the credentials near expiration, credentials may be renewed or re-issued; or, the credential may be revoked
 422 and/or destroyed. Typically, the Subscriber authenticates to the CSP using his or her existing, unexpired
 423 token and credential in order to request re-issuance of a new token and credential. If the Subscriber fails to
 424 request token and credential re-issuance prior to their expiration or revocation, he or she may be required to
 425 repeat the registration process to obtain a new token and credential. The CSP may choose to accept a request
 426 during a grace period after expiration.

427



428
 429

430 Figure 1 - The NIST SP 800-63-1 E-Authentication Architectural Model

⁶ Many assertion protocols require assertions to be forwarded through the Claimant’s local system before reaching the Relying Party. For Details, see Section 10.

431

432 **4.2. Subscribers, Registration Authorities and Credential Service Providers**

433 The previous section introduced the different participants in the conceptual e-authentication model. This
434 section provides additional details regarding the relationships and responsibilities of the participants involved
435 with Registration, Credential Issuance and Maintenance (see the box on the left hand side of Figure 1).

436 A user may be referred to as the Applicant, Subscriber, or Claimant, depending on the stage in the lifecycle
437 of the credential. An Applicant requests credentials from a CSP. If the Applicant is approved and credentials
438 are issued by a CSP, the user is then termed a Subscriber of that CSP. A user may be a Subscriber of
439 multiple CSPs to obtain appropriate credentials for different applications. A Claimant participates in an
440 authentication protocol with a Verifier to prove they are the Subscriber named in a particular credential.

441 The CSP establishes a mechanism to uniquely identify each Subscriber, register the Subscriber's tokens, and
442 track the credentials issued to that Subscriber for each token. The Subscriber may be given credentials to go
443 with the token at the time of registration, or credentials may be generated later as needed. Subscribers have a
444 duty to maintain control of their tokens and comply with the responsibilities to the CSP. The CSP (or the RA)
445 maintains registration records for each Subscriber to allow recovery of registration records.

446 There is always a relationship between the RA and CSP. In the simplest and perhaps the most common case,
447 the RA and CSP are separate functions of the same entity. However, an RA might be part of a company or
448 organization that registers Subscribers with an independent CSP, or several different CSPs. Therefore a CSP
449 may have an integral RA, or it may have relationships with multiple independent RAs, and an RA may have
450 relationships with different CSPs as well.

451 Section 5 specifies requirements for the registration, identity proofing and issuance processes.

452 **4.3. Tokens**

453 The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication:

- 454 a) *Something you know* (for example, a password)
- 455 b) *Something you have* (for example, an ID badge or a cryptographic key)
- 456 c) *Something you are* (for example, a fingerprint or other biometric data)

457 Multi-factor authentication refers to the use of more than one of the factors listed above. The strength of
458 authentication systems is largely determined by the number of factors incorporated by the system.
459 Implementations that use two factors are considered to be stronger than those that use only one factor;
460 systems that incorporate all three factors are stronger than systems that only incorporate two of the factors.
461 (As discussed in Section 4.1, other types of information, such as location data or device identity, may be used
462 by an RP or Verifier to reject or challenge a claimed identity, but they are not considered authentication
463 factors.)

464 In e-authentication, the base paradigm is slightly different: the Claimant possesses and controls a token that
465 has been registered with the CSP and is used to prove the bearer's identity. The token contains a secret the

466 Claimant can use to prove that he or she is the Subscriber named in a particular credential.⁷ In e-
467 authentication, the Claimant authenticates to a system or application over a network by proving that he or she
468 has possession and control of a token. The token provides an output called a token authenticator. This output
469 is used in the authentication process to prove that the Claimant possesses and controls the token (refer to
470 Section 6.1 for more details), demonstrating that the Claimant is the person to whom the token was issued.
471 Depending on the type of token, this authenticator may or may not be unique for individual authentication
472 operations.

473 The secrets contained in tokens are based on either *public key pairs* (asymmetric keys) or *shared secrets*.

474 A *public key* and a related private key comprise a public key pair. The *private key* is stored on the token and
475 is used by the Claimant to prove possession and control of the token. A Verifier, knowing the Claimant's
476 public key through some credential (typically a *public key certificate*), can use an authentication protocol to
477 verify the Claimant's identity, by proving that the Claimant has possession and control of the associated
478 private key token.

479 Shared secrets stored on tokens may be either *symmetric keys* or passwords. While they can be used in
480 similar protocols, one important difference between the two is how they relate to the subscriber. While
481 symmetric keys are generally stored in hardware or software that the Subscriber controls, passwords tend to
482 be memorized by the Subscriber. As such, keys are something the Subscriber has, while passwords are
483 something he or she knows. Since passwords are committed to memory, they usually do not have as many
484 possible values as cryptographic keys, and, in many protocols, are vulnerable to network attacks that are
485 impractical for keys. Moreover the entry of passwords into systems (usually through a keyboard) presents
486 the opportunity for very simple keyboard logging attacks, and it may also allow those nearby to learn the
487 password by watching it being entered. Therefore, keys and passwords demonstrate somewhat separate
488 authentication properties (something you have rather than something you know). However, when using
489 either public key pairs or shared secrets, the Subscriber has a duty to maintain exclusive control of his or her
490 token, since possession and control of the token is used to authenticate the Claimant's identity. Token threats
491 are discussed more in Section 6.2.

492 In this document, e-authentication tokens always contain a secret. So, some of the classic authentication
493 factors do not apply directly to e-authentication. For example, an ID badge is *something you have*, and is
494 useful when authenticating to a human (e.g., a guard), but is not a token for e-authentication. Authentication
495 factors classified as *something you know* are not necessarily secrets, either. Knowledge based authentication,
496 where the claimant is prompted to answer questions that can be confirmed from public databases, also does
497 not constitute an acceptable secret for e-authentication. More generally, *something you are* does not
498 generally constitute a secret. Accordingly, this recommendation does not permit the use of biometrics as a
499 token.

500 However, this recommendation does accept the notional model that authentication systems that incorporate
501 all three factors offer better security than systems that only incorporate two of the factors. An e-
502 authentication system may incorporate multiple factors in either of two ways. The system may be
503 implemented so that multiple factors are presented to the Verifier, or some factors may be used to protect a
504 secret that will be presented to the Verifier. If multiple factors are presented to the Verifier, each will need to

⁷ The stipulation that every token contains a secret is specific to these E-authentication guidelines. As noted elsewhere authentication techniques where the token does not contain a secret may be applicable to authentication problems in other environments (e.g., physical access).

505 be a token (and therefore contain a secret). If a single factor is presented to the Verifier, the additional
506 factors are used to protect the token and need not themselves be tokens.

507 For example, consider a piece of hardware (the token) which contains a cryptographic key (the token secret)
508 where access is protected with a fingerprint. When used with the biometric, the cryptographic key produces
509 an output (the token authenticator) which is used in the authentication process to authenticate the Claimant.
510 An impostor must steal the encrypted key (by stealing the hardware) and replicate the fingerprint to use the
511 token. This specification considers such a device to effectively provide two factor authentication, although
512 the actual authentication protocol between the Verifier and the Claimant simply proves possession of the key.

513 As noted above, biometrics do not constitute acceptable secrets for e-authentication, but they do have their
514 place in this specification. Biometric characteristics are unique personal attributes that can be used to verify
515 the identity of a person who is physically present at the point of verification. They include facial features,
516 fingerprints, DNA, iris and retina scans, voiceprints and many other characteristics. This publication
517 recommends that biometrics be used in the registration process for higher levels of assurance to later help
518 prevent a Subscriber who is registered from repudiating the registration, to help identify those who commit
519 registration fraud, and to unlock tokens.

520 Section 6 provides guidelines on the various types of tokens that may be used for electronic authentication.

521 **4.4. Credentials**

522 As described in the preceding sections, e-authentication credentials bind a token to the Subscriber's name as
523 part of the issuance process. Credentials are issued and maintained by the CSP; Verifiers use the credentials
524 to authenticate the Claimant's identity based on possession and control of the corresponding token. This
525 section provides additional background regarding the relationship of credentials in the e-authentication model
526 with traditional (paper) credentials and describes common e-authentication credentials.

527 Paper credentials are documents that attest to the identity or other attributes of an individual or entity called
528 the subject of the credentials. Some common paper credentials include passports, birth certificates, driver's
529 licenses, and employee identity cards. The authenticity of paper credentials is established in a variety of
530 ways: traditionally perhaps by a signature or a seal, special papers and inks, high quality engraving, and
531 today by more complex mechanisms, such as holograms, that make the credentials recognizable and difficult
532 to copy or forge. In some cases, simple possession of the credentials is sufficient to establish that the physical
533 holder of the credential is indeed the subject of the credentials. More commonly, the credentials contain
534 information such as the subject's description, a picture of the subject or the handwritten signature of the
535 subject, which can be used to authenticate that the holder of the credentials is indeed the subject of the
536 credentials. When these paper credentials are presented in-person, the information contained in those
537 credentials can be checked to verify that the physical holder of the credential is the subject.

538 E-authentication credentials may be considered the electronic analog to paper credentials. In both cases, a
539 valid credential authoritatively binds an identity to the necessary information for verifying that a person is
540 entitled to claim that identity. However, the use cases differ in several significant aspects.

541 The Subject simply possesses and presents the paper credentials in most authentication scenarios. Since they
542 are generally easy to copy, mere possession of a valid electronic credential is rarely a sufficient basis for
543 successful authentication. The e-authentication Claimant possesses a token and presents a token
544 authenticator, but is not necessarily in possession of the electronic credentials. For example, password
545 database entries are considered to be credentials for the purpose of this document but are possessed by the

546 Verifier. X.509 public key certificates are a classic example of credentials the Claimant can (and often does)
547 possess.

548 As was the case for paper credentials, in order to authenticate a Claimant using an electronic credential, the
549 Verifier shall also validate the credential itself (i.e. confirm that the credential was issued by an authorized
550 CSP and has not subsequently expired or been revoked.) There are two ways this can be done: If the
551 credential has been signed by the CSP, the verifier can validate it by checking the signature. Otherwise,
552 validation may be done interactively by querying the CSP directly through a secure protocol.

553 In the remainder of this document, the term “credentials” refers to electronic credentials unless explicitly
554 noted. Section 7 provides guidelines for token and credential management activities that are applicable to
555 electronic authentication.

556 **4.5. Authentication Process**

557 The authentication process begins with the Claimant demonstrating possession and control of a token that is
558 bound to the asserted identity to the Verifier through an authentication protocol. Once possession and control
559 has been demonstrated, the Verifier verifies that the credential remains valid, usually by interacting with the
560 CSP.

561 The exact nature of the interaction between the Verifier and the Claimant during the authentication protocol
562 is extremely important in determining the overall security of the system. Well-designed protocols can protect
563 the integrity and confidentiality of traffic between the Claimant and the Verifier both during and after the
564 authentication exchange, and it can help limit the damage that can be done by an Attacker masquerading as a
565 legitimate Verifier. Additionally, mechanisms located at the Verifier can mitigate online guessing attacks
566 against lower entropy secrets like passwords and PINs by limiting the rate at which an Attacker can make
567 authentication attempts or otherwise delaying incorrect attempts. (Generally, this is done by keeping track of
568 and limiting the number of unsuccessful attempts, since the premise of an online guessing attack is that most
569 attempts will fail.)

570 The Verifier is a functional role, but is frequently implemented in combination with the CSP and/or the RP.
571 If the Verifier is a separate entity from the CSP, it is often desirable to ensure that the Verifier does not learn
572 the subscriber’s token secret in the process of authentication, or at least to ensure that the Verifier does not
573 have unrestricted access to secrets stored by the CSP.

574 Section 8 provides guidelines for the various types of protocols used by the Verifier to authenticate the
575 Claimant/Subscriber within the e-authentication model.

576 **4.6. Assertions**

577 Upon completion of the authentication process, the Verifier generates an assertion containing the result of the
578 authentication and provides it to the RP. If the Verifier is implemented in combination with the RP, the
579 assertion is implicit. If the Verifier is a separate entity from the RP, the assertion is used to pass information
580 about the Claimant or the authentication process from the Verifier to the RP. Assertions may be
581 communicated directly to the RP, or can be forwarded through the Claimant, which has further implications
582 for system design.

583 An RP trusts an assertion based on the source, the time of creation, and attributes associated with the
584 Claimant. The Verifier is responsible for providing a mechanism by which the integrity of the assertion can

585 be confirmed. The RP is responsible for authenticating the source (the Verifier) and for confirming the
586 integrity of the assertion. When the Verifier passes the assertion through the Claimant, the Verifier shall
587 protect the integrity of the assertion in such a way that it cannot be modified by the Claimant. However, if
588 the Verifier and the RP communicate directly, a protected session may be used to provide the integrity
589 protection. When sending assertions across an open network, the Verifier is responsible for ensuring that any
590 sensitive Subscriber information contained in the assertion can only be extracted by an RP that it trusts to
591 maintain the information’s confidentiality.

592 Examples of assertions include:

- 593 a) *Cookies* – Cookies are character strings, placed in memory, which are available to websites within
594 the same Internet domain as the server that placed them in the web browser. Cookies are used for
595 many purposes and may be assertions or may contain pointers to assertions.⁸
- 596 b) *SAML Assertions* – SAML assertions are specified using a mark-up language intended for
597 describing security assertions. They can be used by a Verifier to make a statement to an RP about
598 the identity of a Claimant. SAML assertions may optionally be digitally signed.
- 599 c) *Kerberos Tickets* – Kerberos Tickets allow a ticket granting authority to issue session keys to two
600 authenticated parties using symmetric key based encapsulation schemes.

601 Section 9 provides guidelines for the use of assertions in authentication protocols.

602 **4.7. Relying Parties**

603 An RP relies on results of an electronic authentication protocol to establish confidence in the identity or
604 attributes of a Subscriber for the purpose of some transaction. RPs will use a Subscriber’s authenticated
605 identity, the overall authentication assurance level, and other factors to make access control or authorization
606 decisions. The Verifier and the RP may be the same entity, or they may be separate entities. If they are
607 separate entities, the RP normally receives an assertion from the Verifier. The RP ensures that the assertion
608 came from a Verifier trusted by the RP. The RP also processes any additional information in the assertion,
609 such as personal attributes or expiration times.

610 Section 9 provides guidelines for the assertions that may be used by RPs to establish confidence in the
611 identities of Claimants when the RP and the Verifier are not co-located.

612 **4.8. Calculating the Overall Authentication Assurance Level**

613 The overall authentication assurance level is based on the low watermark of the assurance levels for each of
614 the components of the architecture. For instance, to achieve an overall assurance level of 3:

- 615 a) The registration and identity proofing process shall, at a minimum, use Level 3 processes or
616 higher.
- 617 b) The token (or combination of tokens) used shall have an assurance level of 3 or higher.

⁸ There are specific requirements that agencies must follow when implementing cookies. See OMB Memorandum M-10-22, OMB Guidance for Online Use of Web Measurement and Customization Technologies, available at: http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf as well as OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, available at: <http://www.whitehouse.gov/omb/memoranda/m03-22.html>.

- 618 c) The binding between the identity proofing and the token(s), if proofing is done separately from
619 token issuance, shall be established at level 3.
- 620 d) The authentication protocols used shall have a Level 3 assurance level or higher.
- 621 e) The token and credential management processes shall use a Level 3 assurance level or higher.
- 622 f) Authentication assertions (if used) shall have a Level 3 assurance or higher.

623 The low watermark is the basis for the overall level because the lowest level will likely be the target of the
624 Attacker. For example, if a system uses a token for authentication that has Level 2 assurance, but uses other
625 mechanisms that have Level 3 assurance, the Attacker will likely focus on gaining access to the token since it
626 is easier to attack a system component meeting assurance Level 2 rather than attacking those meeting
627 assurance Level 3. (See Sections 5 through 9 for information on assurance levels for each area.)

628

629 *[KI-IAF: In the following extensions clear requirements from SP 800-63-2 are assessed for equivalence with*
630 *the Service (CSP) Assessment Criteria v3.0 of the Kantara Identity Assurance Framework (at the time of*
631 *writing, in the expectation that there will be produced a SAC v4.0 containing, at least, revisions to reflect*
632 *these mappings).*

633 *References to mapped (i.e. comparable) criteria are recorded with any commentary where required.]*

634

635 5. Registration and Issuance Processes

636 5.1. Overview

637 5.1.1 In the registration process, an Applicant undergoes identity proofing by a trusted RA. If the RA is
638 able to verify the Applicant’s identity, the CSP registers or gives the Applicant a token and issues a credential
639 as needed to bind that token to the identity or some related attribute. The Applicant is now a Subscriber of the
640 CSP and may use the token as a Claimant in an authentication protocol. This section describes the
641 requirements for registration and for token and credential issuance.

642 5.1.2 The RA can be a part of the CSP, or the RA can be a separate and independent entity; however, a
643 trusted relationship always exists between the RA and CSP. Where the RA and CSP are separate entities, the
644 trust relationship is often contractual, but the trust relationship may also be based on laws and regulations,
645 such as when a notary performs the RA function. The RA or CSP maintain records of the registration. The
646 RA and CSP can provide services on behalf of an organization or may provide services to the public. The
647 processes and mechanisms available to the RA for identity proofing may differ as a result. Where the RA
648 operates on behalf of an organization, the identity proofing process may be able to leverage a pre-existing
649 relationship (e.g., the Applicant is an employee or student). Where the RA provides services to the public, the
650 identity proofing process is generally limited to confirming publicly available information and previously
651 issued credentials.

652 5.1.3 The registration and identity proofing processes are designed based on the required assurance level,
653 to ensure that the RA/CSP knows the true identity of the Applicant. Specifically, the requirements include
654 measures to ensure that:

- 655 a) A person with the Applicant’s claimed attributes exists, and those attributes are sufficient to
656 uniquely identify a single person;
- 657 b) The Applicant whose token is registered is in fact the person who is entitled to the identity;
- 658 c) It is difficult for the Claimant to later repudiate the registration and dispute an authentication
659 using the Subscriber’s token.

660 5.1.4 An Applicant may appear in person to register, or the Applicant may register remotely. Somewhat
661 different processes and mechanisms apply to identity proofing in each case. Remote registration is limited to
662 Levels 1 through 3.

663 5.1.5 After successful identity proofing of the Applicant, the RA registers the Applicant, and then the CSP
664 is responsible for token and credential issuance for the new Subscriber (additional CSP responsibilities are
665 discussed further in Section 7). Issuance includes creation of the token. Depending on the type of token
666 being used, the CSP will either create a new token and supply the token to the Subscriber, or require the
667 Subscriber to register a token that the Applicant already possesses or has newly created. In either case, the
668 mechanism for transporting the token from the token origination point to the Subscriber may need to be
669 secured to ensure that the confidentiality and integrity of the newly established token is maintained and that
670 token is in possession of correct Applicant.

671 5.1.6 The CSP is also responsible for the creation of a credential that binds the Subscriber’s identity to his
672 or her token. Optionally, the CSP may include other verified attributes about the Subscriber within the
673 credential, such as his or her organizational affiliation, policies, or constraints for token use.

674 **5.1.7** In models where the registration and identity proofing take place separately from credential
 675 issuance, the CSP is responsible for verifying that the credential is being issued to the same person who was
 676 identity proofed by the RA. In this model, issuance must be strongly bound to registration and identity
 677 proofing so that an Attacker cannot pose as a newly registered Subscriber and attempt to collect a
 678 token/credential meant for the actual Subscriber. This attack, and similar attacks, can be thwarted by the
 679 methods described in Section 5.3.1, which describes which techniques are considered appropriate for
 680 establishing the necessary binding at the various assurance levels.

681 **5.2. Registration and Issuance Threats**

682 **5.2.1. Overview**

683 There are two general categories of threats to the registration process: impersonation and either compromise
 684 or malfeasance of the infrastructure (RAs and CSPs). This recommendation concentrates on addressing
 685 impersonation threats. Infrastructure threats are addressed by normal computer security controls (e.g.,
 686 separation of duties, record keeping, independent audits) and are outside the scope of this document⁹.
 687 [*KI-IAF: similarly, it is considered that any attempt to map to NIST SP 800-53 controls is out of scope.*]

688 The threats to the issuance process include impersonation attacks and threats to the transport
 689 mechanism for the token and credential issuance.
 690 Table 1 lists the threats related to registration and issuance.

691
 692

Table 1 - Registration and Issuance Threats

Activity	Threat/Attack	Example
Registration ¹⁰	Impersonation of claimed identity	An Applicant claims an incorrect identity by using a forged driver's license.
	Repudiation of registration	A Subscriber denies registration, claiming that he or she did not register that token.
Issuance	Disclosure	A key created by the CSP for a Subscriber is copied by an Attacker as it is transported from the CSP to the Subscriber during token issuance.
	Tampering	A new password created by the Subscriber is modified by an Attacker as it is being submitted to the CSP during the credential issuance phase.
	Unauthorized issuance	A person claiming to be the Subscriber (but in reality is not the Subscriber) is issued credentials for that Subscriber.

693 **5.2.2. Threat Mitigation Strategies**

694 Registration threats can be deterred by making impersonation more difficult to accomplish or increasing the

⁹ See NIST SP800-53, *Recommended Security Controls For Federal Information Systems* for appropriate security controls.

¹⁰ Some impostors may attempt to register as any Subscriber in the system and other impostors may wish to register as a specific Subscriber.

695 likelihood of detection. This recommendation deals primarily with methods for making impersonation more
 696 difficult; however, it does prescribe certain methods and procedures that may help to prove who carried out
 697 an impersonation. At each level, methods are employed to determine that a person with the claimed identity
 698 exists, that the Applicant is the person who is entitled to the claimed identity, and that the Applicant cannot
 699 later repudiate the registration. As the level of assurance increases, the methods employed provide increasing
 700 resistance to casual, systematic and insider impersonation. Table 2 lists strategies for mitigating threats to the
 701 registration and issuance processes.
 702

703 Table 2 - Registration and Issuance Threat Mitigation Strategies

Activity	Threat/Attack	Mitigation Strategy
Registration	Impersonation of claimed identity	RAs request documentation that provides a specified level of confidence (or assurance) in the identity of the Applicant and makes it more difficult for imposters to successfully pass the identity proofing step.
		Government issued documents such as driver's licenses, and passports presented by the Applicant are often used to assert the identity of the Applicant.
	Have the Applicant provide non-government issued documentation (e.g. electricity bills in the name of the Applicant with the current address of the Applicant printed on the bill, or a credit card bill) to help in achieving a higher level of confidence in the identity of the Applicant.	
	Repudiation of registration	Have the Applicant sign a form acknowledging participation in the registration activity.
Issuance	Disclosure	Issue the token in person, physically mail it in a sealed envelope to a secure location, or use a protected session to send the token electronically.
	Tampering	Issue credentials in person, physically mailing storage media in a sealed envelope, or through the use of a communication protocol that protects the integrity of the session data.
		Establish a procedure that allows the Subscriber to authenticate the CSP as the source of any token and credential data that he or she may receive.
	Unauthorized issuance	Establish procedures to ensure that the individual who receives the token is the same individual who participated in the registration procedure.

Activity	Threat/Attack	Mitigation Strategy
		Implement a dual-control issuance process that ensures two independent individuals shall cooperate in order to issue a token and/or credential.

704
705

706 **5.3. Registration and Issuance Assurance Levels**

707 The following sections list the NIST recommendations for registration and issuance for the four levels
 708 corresponding to the OMB guidance. As noted in the OMB guidance, Levels 1 and 2 recognize the use of
 709 pseudonymous credentials. When pseudonymous credentials are used to imply membership in a group, the
 710 level of proofing shall be consistent with the requirements for the credential of that level. Explicit
 711 requirements for registration processes for pseudonymous credentials are not specified, as they are unique to
 712 the membership criteria for each specific group.

713 **5.3.1. General Requirements per Assurance Level**

714 *[KI-IAF: The treatment of requirements at the differing LoAs is very disjointed in this section of the original*
 715 *document and therefore difficult to map. To address this:*

- 716 *a) the text has been restructured to provide clear requirements for each level;*
- 717 *b) re-phrasing has been applied to remove the explicit ‘at Level x’ qualifications, however;*
- 718 *c) in this draft NIST’s original ‘level-qualifying’ text has been retained in italics as a lead-in so as to*
 719 *illustrate the rationale for inclusion (or not) of any particular text from the original material;*
- 720 *d) in order to maintain a one-one relationship throughout with sub-clause numbering, where higher ALs*
 721 *impose additional requirements, some sub-clauses at lower ALs are void of meaningful*
 722 *requirements.*

723
 724 *The Table 3 below provides a mapping of the re-structured text in this section to the contents of the original*
 725 *Table 3.]*

726 **Table 3 - Identity Proofing Requirements by Assurance Level**

	In-Person	Remote
Level 2		
Basis for issuing credentials	5.3.1.2.11 a)	5.3.1.2.11 c)
RA and CSP actions	5.3.1.2.11 b)	5.3.1.2.11 d)
Level 3		
Basis for issuing credentials	5.3.1.3.11 a)	5.3.1.3.11 c)
RA and CSP actions	5.3.1.3.11 b)	5.3.1.3.11 d)
Level 4		
Basis for issuing credentials	5.3.1.4.11 a)	Not permitted
RA and CSP actions	5.3.1.4.11 b)	Not permitted

727

728

729 **5.3.1.1. Registration and Issuance at Level 1**

730 5.3.1.1.1 to 5.3.1.1.4 No stipulation.

731 5.3.1.1.5 All ... The CSP shall:

732 a) be able to uniquely identify each Subscriber and the associated tokens and the credentials issued
733 to that Subscriber;

734 [KI-IAF: AL1_ID_POL#010, AL1_ID_POL#020, AL1_CM_CRN#030]

735 b) be capable of conveying this information to Verifiers;

736 [KI-IAF: AL1_ID_VRC#025, AL1_CM_CRN#-035]

737 c) ensure that the name associated with the Subscriber is provided by the Applicant and accepted
738 without verification.

739 [KI-IAF: AL1_ID_IPV#010, AL1_ID_IPV#020]

740 5.3.1.1.6 to 5.3.1.1.8 No stipulation.

741 5.3.1.1.9 At all levels ... Personally identifiable information (PII) collected as part of the registration
742 process shall be protected, and all privacy requirements shall be satisfied.

743 [KI-IAF: AL1_CO_ESM#050, AL1_CO_ESM#055]

744 5.3.1.1.10 No further stipulations.

745

746 **5.3.1.2. Registration and Issuance at Level 2**

747 5.3.1.2.1 For levels 2 and above ... Records of registration shall be maintained either by the RA or by the
748 CSP, depending on the context. Either the RA or the CSP shall maintain a record of each individual whose
749 identity has been verified and the steps taken to verify his or her identity, including any information collected
750 from the applicant in compliance with the sections below.

751 [KI-IAF: AL2_ID_VRC#010, AL2_ID_VRC#020, AL2_ID_VRC#030]

752 5.3.1.2.2 For levels 2 and above ... The CSP shall have the capability to provide records of identity
753 proofing to RPs if required, to the extent permitted by applicable legislation and/or agreed by the
754 Subscriber¹¹.

755 [KI-IAF: AL2_CO_ESM#050 (oblique reference to understanding legislation), AL2_ID_VRC#025]

756 5.3.1.2.3 For levels 2 and above ... The identity proofing and registration processes shall be performed
757 according to an applicable written policy or *practice statement* that specifies the particular steps taken to
758 verify identities.

759 [KI-IAF: AL2_CO_NUI#020 a), AL2_ID_POL#030, AL2_ID_POL#040, AL2_ID_IDV#010]

760 5.3.1.2.4 For levels 2 and above ... If the RA and CSP are remotely located and communicate over a
761 network, the entire registration transaction between the RA and CSP shall occur over a mutually-
762 authenticated protected session. **Equivalently**[KI-IAF: *Alternatively?*], the transaction may consist of time-
763 stamped or sequenced messages signed by their source and encrypted for their recipient. In either case,
764 approved cryptography is required.

765 [KI-IAF: AL2_CO_]

766

¹¹ It is beyond the scope of this document to specify what circumstances make it necessary and/or appropriate for the CSP to provide this information. Refer to applicable privacy laws, rules of evidence etc.

- 767 5.3.1.2.5 All ... The CSP shall:
- 768 a) be able to uniquely identify each Subscriber and the associated tokens and the credentials issued
769 to that Subscriber;
770 [KI-IAF: AL2_ID_POL#010, AL2_ID_POL#020, AL2_CM_CRN#020, AL2_CM_CRN#030]
- 771 b) be capable of conveying this information to Verifiers.
772 [KI-IAF: AL2_ID_VRC#025, AL2_CM_CRN#035]
- 773 ~~ensure that the name associated with the Subscriber is provided by the Applicant and accepted~~
774 ~~without verification.~~
775 [KI-IAF: this makes no sense at AL2 and above –63-2 needs to be modified (Burr concurred on
776 this point)]
- 777 5.3.1.2.6 At Level 2 ... The identifier associated with the Subscriber may be pseudonymous but the RA or
778 CSP shall retain the actual identity of the Subscriber.
779 [KI-IAF: AL2_CM_CRN#090, AL2_CM_CRN#095]
- 780 5.3.1.2.7 At Level 2 ... Pseudonymous credentials shall be distinguishable from credentials that contain
781 verified names.
782 [KI-IAF: AL2_CM_CRN#090, AL2_CM_CRN#095]
- 783 5.3.1.2.8 No stipulation.
- 784 5.3.1.2.9 At all levels ... Personally identifiable information (PII) collected as part of the registration
785 process shall be protected, and all privacy requirements shall be satisfied.
786 [KI-IAF: AL2_CO_ESM#050, AL2_CO_ESM#055]
- 787 5.3.1.2.10 for Levels 2 and 3 ... Both in-person and remote registration are permitted. Remote registration
788 requirements are designed to permit fully-automated solutions. However, implementations may also
789 leverage call centers or online assistance as a substitute or complement for fully-automated solutions.
790 [KI-IAF: AL2_ID_IDV#000 - NOTE – KI also allows 'current relationship' and 'affiliation' (both antecedent). These are
791 considered to be addressed by §5.3.2 and hence are US Profiling.
792 AL2_IDV_SCV#010]
- 793 5.3.1.2.11 At Level 2 and higher ... For an *ab initio* application, the Applicant supplies his or her full legal
794 name, an address of record, and date of birth, and may, subject to the policy of the RA or CSP, also supply
795 other PII. Specifically, at Assurance Level 2¹²:
796 [KI-IAF: from Table 3- Level 2]
- 797 a) For in-person identity-proofing the Applicant must provide:
798 i) valid current primary government picture ID¹³ that contains Applicant's picture; and
799 ii) either address of record or nationality of record (e.g., driver's license or Passport).
800 [KI-IAF: AL2_ID_IPV#010+NIST SP 800-63-2 Profiling]
801 [KI-IAF: SP800-63-2 goes further than the KIAF requirements (which address a) i) only), but one has to ask
802 whether it is reasonable to directly impose upon all parties such requirements derived from 63-2 or whether it is
803 preferable to regard them as a national-specific profiling, which is the approach taken in this draft and which should

¹² A token at this Level may also be obtained by authenticating to the CSP using mechanisms at the same or a higher Level (e.g., PIV). See 5.3.5 for more information.

¹³ The following resources offer examples of what some agencies consider to be primary or secondary ID:

- USCIS Form I-9, "Lists of Acceptable Documents", <http://www.uscis.gov/files/form/i-9.pdf>
- Instructions for First Time Passport Applicants http://travel.state.gov/passport/get/first/first_830.html#step4first
- Secondary Evidence of Identification http://travel.state.gov/passport/get/secondary_evidence/secondary_evidence_4314.html

804
805

be assumed from hereon whenever the phrase “NIST SP 800-63-2 Profiling” is encountered, i.e. services not seeking to meet US Federal requirements may employ alternative approaches which have equivalent rigour.]

806
807

- b) For in-person identity-proofing the RA (or CSP, as applicable) must:

[KI-IAF: AL2_ID_IDV#010 +NIST SP 800-63-2 Profiling]

808

- i) inspect photo-ID; compare picture to Applicant; and record the ID number, address and date of birth (DoB);

809

[KI-IAF: AL2_ID_IPV#020 a, b) +NIST SP 800-63-2 Profiling]

810

811

- ii) review any additionally-required personal information in records necessary to support issuance process;

812

[KI-IAF: AL2_ID_SCV#010 +NIST SP 800-63-2 Profiling]

813

814

- iii) issue a credential by performing one of the following actions:

815

- 1) if personal information in records includes a telephone number or e-mail address, the CSP issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records; or

816

817

818

- 2) if ID confirms address of record, RA authorizes or CSP issues credentials. Notice is sent to address of record; or

819

820

- 3) if ID does not confirm address of record, CSP issues credentials in a manner that confirms the claimed address.

821

822

823

[KI-IAF: AL2_ID_RPV#020 d, e, f), AL2_CM_CRD#010 +NIST SP 800-63-2 Profiling]

824

- c) For remote identity-proofing the Applicant must demonstrate:

825

- i) possession of a valid current government ID¹⁴ (e.g., a driver’s license or Passport) number; and

826

827

- ii) a financial or utility account number (e.g. checking account, savings account, utility account, loan or credit card, or tax ID) or a telephone service account;

828

829

[KI-IAF: AL2_ID_RPV#010 +NIST SP800-63-2 Profiling]

830

831

- d) For remote identity-proofing the RA (or CSP, as applicable) must:

832

[KI-IAF: AL2_ID_IDV#010 +NIST SP 800-63-2 Profiling]

833

- i) confirm via records either the government ID or the account number;

834

Note that confirmation of the financial or utility account may require supplemental information from the applicant.

835

[KI-IAF: AL2_ID_RPV#020 a, b) +NIST SP 800-63-2 Profiling, AL2_ID_SCV#010]

836

837

838

- ii) inspect both ID number and account number supplied by Applicant (e.g., for correct

839

format & number of digits);

840

[KI-IAF: AL2_ID_RPV#020 +NIST SP 800-63-2 Profiling, AL2_ID_SCV#010]

841

842

- iii) Verify information provided by Applicant including ID number OR account number

843

through record checks either with the applicable agency or institution or through credit bureaus or similar databases;

844

[KI-IAF: AL2_ID_RPV#020 a, b) +NIST SP 800-63-2 Profiling, AL2_ID_SCV#010]

845

846

847

- iv) confirms that: name, DoB, address and other personal information in records are on

848

balance consistent with the application and sufficient to identify a unique individual;

849

[KI-IAF: AL2_ID_RPV#020 a, b) +NIST SP 800-63-2 Profiling, AL2_ID_SCV#010]

850

¹⁴ Agencies issuing credentials to foreign nationals residing in foreign countries determine what constitutes a valid Government issued ID as required.

- 851 v) for utility account numbers, confirmation shall be performed by verifying knowledge of
852 recent account activity. (This technique may also be applied to some financial
853 accounts.);
854 [KI-IAF: AL2_ID_RPV#020 c) +NIST SP 800-63-2 Profiling, AL2_ID_SCV#010]
855
- 856 vi) for telephone service accounts, confirmation that the phone number is associated in
857 Records with the Applicant's name and address of record and by having the applicant
858 demonstrate that they are able to send or receive messages at the phone number;
859 [KI-IAF: AL2_ID_RPV#020 d]
860
- 861 vii) Confirm address/phone number/email by issuing a credential by performing one of the
862 following actions¹⁵:
863 1) CSP issues credentials in a manner that confirms the ability of the Applicant to
864 receive mail at a physical address associated with the Applicant in records; or
865 2) If personal information in records includes a telephone number or e-mail address,
866 the CSP issues credentials in a manner that confirms the ability of the Applicant to
867 receive telephone communications or text message at phone number or e-mail
868 address associated with the Applicant in records; or
869 3) CSP issues credentials: RA or CSP sends notice to an address of record confirmed
870 in the records check.¹⁶
871 [KI-IAF: AL2_ID_RPV#020 e, f, g]
- 872 viii) Any secret sent over an unprotected session shall be reset upon first use and shall be
873 valid for a maximum lifetime of seven days.
874 [KI-IAF: AL2_ID_RPV#020 h]
875

876 **5.3.1.2.12** All ... If a valid credential has already been issued at Level 2 or higher, the CSP may issue
877 another credential at Level 1 or 2. In this case, proof of possession and control of the original token may be
878 substituted for repeating the identity proofing steps. (This is a special case of a derived credential. See
879 Section 5.3.5 for procedures when the derived credential is issued by a different CSP.) Any requirements for
880 credential delivery defined at §0 b) or d) (as applicable) shall still be satisfied.
881 [KI-IAF: AL2_ID_IDC#010 +NIST SP 800-63-2 Profiling]

882 **5.3.1.2.13** At Level 2 and higher ... Sensitive data collected during the registration and identity proofing
883 stage shall be protected during transmission and storage so as to ensure their security and confidentiality.
884 [KI-IAF: AL2_CO_ESM#050, AL2_CO_SCO#010]

885 **5.3.1.2.14** At Level 2 and higher ... Additionally, the results of the identity proofing step (which may
886 include background investigations of the Applicant) have to be protected to ensure source document
887 authentication, confidentiality, and integrity.
888 [KI-IAF: AL2_CO_ESM#050, AL2_CO_SCO#010]

889 890 **5.3.1.3. Registration and Issuance at Level 3**

891 **5.3.1.3.1** As Level 2 (see 5.3.1.2.1).
892 [KI-IAF: AL3_ID_VRC#010, AL3_ID_VRC#020, AL3_ID_VRC#030]

¹⁵ Requirements that use USPS mail for address confirmation and/or notification have a legal basis: Title 18 U.S. Code: Criminal Procedure, Section 1708: Theft or receipt of stolen mail matter generally.

¹⁶ Agencies are encouraged to use methods 1) and 2) where possible to achieve better security. Method 3) is especially weak when not used in combination with knowledge of account activity.

- 893 5.3.1.3.2 As Level 2 (see 5.3.1.2.2).
894 [KI-IAF: AL3_CO_ESM#050 (oblique reference to understanding legislation), AL3_ID_VRC#025]
- 895 5.3.1.3.3 As Level 2 (see 5.3.1.2.3).
896 [KI-IAF: AL3_CO_NUI#020 a), AL3_ID_POL#030, AL3_ID_POL#040, AL3_ID_IDV#010]
- 897 5.3.1.3.4 As Level 2 (see 5.3.1.2.4).
898 [KI-IAF: AL3_CO_SCO#010]
- 899 5.3.1.3.5 All ... The CSP shall:
- 900 a) be able to uniquely identify each Subscriber and the associated tokens and the credentials issued
901 to that Subscriber;
902 [KI-IAF: AL3_ID_POL#010, AL3_ID_POL#020, AL3_CM_CRN#020, AL3_CM_CRN#030]
- 903 b) be capable of conveying this information to Verifiers.
904 [KI-IAF: AL3_CO_VRC#025, AL3_CM_CRN#035]
- 905 c) ~~ensure that the name associated with the Subscriber is provided by the Applicant and accepted~~
906 ~~without verification.~~
907 [KI-IAF: this makes no sense at AL2 and above – 800-63 needs to be modified (Burr concurred
908 on this point)]
- 909 5.3.1.3.6 to 5.3.1.3.7 No stipulation.
- 910 5.3.1.3.8 At Level 3 and above ... The name associated with the Subscriber shall be verified.
911 [KI-IAF: AL3_ID_IPV#020, AL3_ID_RPV#020, AL3_ID_AFV#020]
- 912 5.3.1.3.9 At all levels ... Personally identifiable information (PII) collected as part of the registration
913 process shall be protected, and all privacy requirements shall be satisfied.
914 [KI-IAF: AL3_CO_ESM#050, AL3_CO_ESM#055]
- 915 5.3.1.3.10 As Level 2.
916 [KI-IAF: AL3_ID_IDV#000 - NOTE – KI also allows ‘current relationship’ and ‘affiliation’ (antecedent). These are considered
917 to be addressed by §5.3.2 and hence are US Profiling.
918 AL3_IDV_SCV#010]
- 919 5.3.1.3.11 At Level 2 and higher ... For an *ab initio* application, the Applicant supplies his or her full legal
920 name, an address of record, and date of birth, and may, subject to the policy of the RA or CSP, also supply
921 other PII. Specifically, at Assurance Level 3¹²:
922 [KI-IAF: from Table 3- Level 3]
- 923 a) For in-person identity-proofing the Applicant must provide:
924 i) valid current primary government picture ID that contains Applicant’s picture; and
925 ii) either address of record or nationality of record (e.g., driver’s license or Passport.
926 [KI-IAF: AL3_ID_IPV#010 +NIST SP 800-63-2 Profiling]
- 927 b) For in-person identity-proofing the RA (or CSP, as applicable) must:
928 [KI-IAF: AL3_ID_IDV#010 +NIST SP 800-63-2 Profiling]
- 929 i) inspect photo-ID; compare picture to Applicant; and record the ID number, **address and**
930 **date of birth (DoB)** [KI-IAF: This inclusion agreed by Burr to be an omission in 63-2];
931 [KI-IAF: AL3_ID_IPV#020 a, b) +NIST SP 800-63-2 Profiling]
- 932 ii) verify the photo-ID via the issuing government agency or through credit bureaus or
933 similar databases. Confirm that: name, DoB, address and other personal information in
934 record are consistent with the application;
935 [KI-IAF: AL3_ID_IPV#020 +NIST SP 800-63-2 Profiling]

- 936 iii) issue a credential by performing one of the following actions:
937 1) if personal information in records includes a telephone number, the CSP issues
938 credentials in a manner that confirms the ability of the Applicant to receive
939 telephone communications at a number associated with the Applicant in records,
940 while recording the Applicant’s voice or using alternative means that establish an
941 equivalent level of non-repudiation; or
942 2) if ID confirms address of record, RA authorizes or CSP issues credentials. Notice
943 is sent to address of record; or
944 3) if ID does not confirm address of record, CSP issues credentials in a manner that
945 confirms the claimed address.
946 [*KI-IAF: AL3_ID_RPV#020 d, e, f), AL3_CM_CRD#010 +NIST SP 800-63-2 Profiling*]
- 947 c) For remote identity-proofing the Applicant must demonstrate:
948 i) possession of a valid current government ID¹⁷ (e.g., a driver’s license or Passport)
949 number; and
950 ii) a financial or utility account number (e.g. checking account, savings account, utility
951 account, loan or credit card, or tax ID) or a telephone service account.
952 [*KI-IAF: AL3_ID_RPV#010 +NIST SP 800-63-2 Profiling*]
- 953 d) For remote identity-proofing the RA (or CSP, as applicable) must:
954 [*KI-IAF: AL3_ID_IDV#010 +NIST SP 800-63-2 Profiling*]
955 i) confirm via records both the government ID or the account number;
956 Note that confirmation of the financial or utility account may require supplemental
957 information from the Applicant.
958 [*KI-IAF: AL3_ID_RPV#020 a, b) +NIST SP 800-63-2 Profiling, AL3_ID_SCV#010*]
959
960 ii) [*KI-IAF: Note that there is no requirement at AL3 which is equivalent to that at AL2 as expressed by*
961 §5.3.1.2.11 d) ii), *although in all good reason there should be. This void clause is included here for the*
962 *sake of alignment between AL2 and AL3 in the mapping with the Kantara SAC.*]
963
964 iii) verify information provided by Applicant including ID number AND account number
965 through record checks either with the applicable agency or institution or through credit
966 bureaus or similar databases. At a minimum, the records check for both the ID number
967 AND the account number should confirm the name and address of the Applicant;
968 [*KI-IAF: AL3_ID_RPV#020 +NIST SP 800-63-2 Profiling, AL3_ID_SCV#010*]
969
970 iv) confirms that: name, DoB, address and other personal information in records are on
971 balance consistent with the application and sufficient to identify a unique individual.;
972 [*KI-IAF: AL3_ID_RPV#020 a, b) +NIST SP 800-63-2 Profiling, AL3_ID_SCV#010*]
973
974 v) For utility account numbers, confirmation shall be performed by verifying knowledge of
975 recent account activity. (This technique may also be applied to some financial
976 accounts.);
977 [*KI-IAF: AL3_ID_RPV#020 c) +NIST SP 800-63-2 Profiling, AL3_ID_SCV#010*]
978
979 vi) for telephone service accounts, confirmation that the phone number is associated in
980 Records with the Applicant's name and address of record and by having the applicant
981 demonstrate that they are able to send or receive messages at the phone number;

¹⁷ Agencies issuing credentials to foreign nationals residing in foreign countries determine what constitutes a valid Government issued ID as required.

[KI-IAF: AL3_ID_RPV#020 d]

- vii) Confirm address/phone number/email by issuing a credential by performing one of the following actions:
- 1) CSP issues credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in records; or¹⁵
 - 2) If personal information in records includes both an electronic address and a physical address that are linked together with the Applicant's name, and are consistent with the information provided by the applicant, then, the CSP may issue credentials in a manner that confirms the ability of the Applicant to receive messages (SMS, voice or e-mail) sent to the electronic address.

[KI-IAF: AL3_ID_RPV#020 e, f, g]

- viii) Any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days.

[KI-IAF: AL3_ID_RPV#020 h]

5.3.1.3.12 All ... If a valid credential has already been issued at Level 3 or 4, the CSP may issue another credential at Level 3 or below. In this case, proof of possession and control of the original token may be substituted for repeating the identity proofing steps. (This is a special case of a derived credential. See Section 5.3.5 for procedures when the derived credential is issued by a different CSP.) Any requirements for credential delivery defined at §5.3.1.3.11 b) or d) (as applicable) shall still be satisfied.

[KI-IAF: AL3_ID_IDC#010 +NIST SP 800-63-2 Profiling]

5.3.1.3.13 At Level 2 and higher ... Sensitive data collected during the registration and identity proofing stage shall be protected during transmission and storage so as to ensure their security and confidentiality.

[KI-IAF: AL3_CO_ESM#050, AL3_CO_SCO#010]

5.3.1.3.14 At Level 2 and higher ... Additionally, the results of the identity proofing step (which may include background investigations of the Applicant) have to be protected to ensure source authentication, confidentiality, and integrity.

[KI-IAF: AL3_CO_ESM#050, AL3_CO_SCO#010]

5.3.1.4. Registration and Issuance at Level 4

5.3.1.4.1 As Level 3 (see 5.3.1.3.1).

[KI-IAF: AL4_ID_VRC#010, AL4_ID_VRC#020, AL4_ID_VRC#030]

5.3.1.4.2 As Level 3 (see 5.3.1.3.2).

[KI-IAF: AL4_CO_ESM#050 (oblique reference to understanding legislation), AL4_ID_VRC#025]

5.3.1.4.3 As Level 3 (see 5.3.1.3.3).

[KI-IAF: AL4_CO_NUI#020 a), AL4_ID_POL#030, AL4_ID_POL#040, AL3_ID_IDV#010]

5.3.1.4.4 As Level 3 (see 5.3.1.3.4).

[KI-IAF: AL4_CO_SCO#010]

5.3.1.4.5 All ... The CSP shall:

- a) be able to uniquely identify each Subscriber and the associated tokens and the credentials issued to that Subscriber;

[KI-IAF: AL4_ID_POL#010, 'POL#020, AL4_CM_CRN#020, AL4_CM_CRN#030]

1026 b) be capable of conveying this information to Verifiers.
1027 [KI-IAF: AL4_ID_VRC#025, AL4_CM_CRN#035]

1028 ~~ensure that the name associated with the Subscriber is provided by the Applicant and accepted~~
1029 ~~without verification.~~ [KI-IAF: Burr confirms that the omission of this requirement in 800-63-2 is an error]

1030 5.3.1.4.9 At all levels ... Personally identifiable information (PII) collected as part of the registration
1031 process shall be protected, and all privacy requirements shall be satisfied.
1032 [KI-IAF: AL4_CO_ESM#050, AL4_CO_ESM#055]

1033 5.3.1.4.10 At Level 4 ... Only in-person registration is permitted.
1034 [KI-IAF: AL4_ID_IDV#000, AL4_IDV_SCV#010]

1035 5.3.1.4.11 At Level 2 and higher ... The Applicant supplies his or her full legal name, an address of record,
1036 and date of birth, and may, subject to the policy of the RA or CSP, also supply other PII. Specifically, at
1037 Assurance Level 4¹²:
1038 [KI-IAF: from Table 3- Level 4]

1039 a) The in-person Applicant must provide:
1040 i) a current primary government picture ID that contains Applicant's picture; and
1041 ii) either address of record or nationality of record (e.g., driver's license or Passport); and
1042 iii) either a second, independent Government ID document that contains current
1043 corroborating information (e.g., either address of record or nationality of record), OR
1044 verification of a financial account number (e.g., checking account, savings account, loan
1045 or credit card) confirmed via records.

1046 [KI-IAF: AL4_ID_IPV#010 +NIST SP 800-63-2 Profiling]

1047 b) The RA (or CSP, as applicable) must:

1048 [KI-IAF: AL4_ID_IDV#010 +NIST SP 800-63-2 Profiling]

1049 i) inspect photo-ID; compare picture to Applicant; and record the ID number, address and
1050 date of birth (DoB); [KI-IAF: Burr confirms that the omission of this requirement in 800-63-2 is an
1051 error]

1052 [KI-IAF: AL4_ID_IPV#030, AL4_ID_IPV#040 +NIST SP 800-63-2 Profiling]

1053
1054 ii) verify the photo-ID via the issuing government agency or through credit bureaus or
1055 similar databases. Confirm that: name, DoB, address and other personal information in
1056 record are consistent with the application;

1057 [KI-IAF: AL4_ID_IPV#030, AL4_ID_IPV#040 +NIST SP 800-63-2 Profiling]

1058
1059 iii) inspect any secondary Government ID provided and if apparently valid, confirm that the
1060 identifying information is consistent with the primary Photo-ID;

1061 [KI-IAF: AL4_ID_IPV#030, AL4_ID_IPV#040 +NIST SP 800-63-2 Profiling]

1062
1063 iv) verify any financial account number supplied by Applicant through record checks or
1064 through credit bureaus or similar databases, and confirm that: name, DoB, address, and
1065 other personal information in records are on balance consistent with the application and
1066 sufficient to identify a unique individual;

1067 [KI-IAF: AL4_ID_IPV#030, AL4_ID_IPV#040 +NIST SP 800-63-2 Profiling]

1068 **Note: Address of record shall be confirmed through validation of either the primary**
1069 **or secondary ID.**

1070
1071 iv) RA shall record a current biometric (e.g., photograph or fingerprints) to ensure that
1072 Applicant cannot repudiate application;

1073 [KI-IAF: AL4_ID_IPV#030, 'AL4_ID_PV#040 +NIST SP 800-63-2 Profiling]

1074

1075 v) issue a credential in a manner that confirms address of record.

1076 [KI-IAF: AL4_CM_CRD#010 +NIST SP 800-63-2 Profiling]

1077

1078 5.3.1.4.12 All ... If a valid credential has already been issued at Level 4, the CSP may issue another
1079 credential at Level 4 or below. In this case, proof of possession and control of the original token may be
1080 substituted for repeating the identity proofing steps. (This is a special case of a derived credential. See
1081 Section 5.3.5 for procedures when the derived credential is issued by a different CSP.) Any requirements for
1082 credential delivery defined at §5.3.1.4.11 b) shall still be satisfied.

1083 [KI-IAF: AL4_ID_IDC#010 +NIST SP 800-63-2 Profiling]

1084 5.3.1.4.13 At Level 2 and higher ... Sensitive data collected during the registration and identity proofing
1085 stage shall be protected during transmission and storage so as to ensure their security and confidentiality.

1086 [KI-IAF: AL4_CO_ESM#050, 'SCO#010]

1087 5.3.1.4.14 At Level 2 and higher ... Additionally, the results of the identity proofing step (which may
1088 include background investigations of the Applicant) have to be protected to ensure source authentication,
1089 confidentiality.

1090 [KI-IAF: AL4_CO_ESM#050, 'SCO#010]

1091

1092 [KI-IAF: The following paragraph appears in SP 800-63-2 §5.3.1 (pg.32) but presents no requirements and
1093 hence is not mapped.]

1094 In some contexts, once an agency has met the minimum registration requirements for an assurance level, the
1095 agency may choose to use additional knowledge based authentication methods to increase confidence in the
1096 registration process. For example, an Applicant could be asked to supply non-public information on his or
1097 her past dealing with the agency that could help confirm the Applicant's identity.

1098

1099 5.3.1.5. Applicant's continuity

1100 5.3.1.5.1 Registration, identity proofing, token creation/issuance, and credential issuance are separate
1101 processes that can be broken up into a number of separate physical encounters or electronic transactions.
1102 (Two electronic transactions are considered to be separate if they are not part of the same protected session.)

1103 5.3.1.5.2 The following methods shall be used to ensure that the same party acts as Applicant
1104 throughout the processes:

1105 a) At Level 1, there is no specific requirement, ~~however some effort should be made to uniquely identify~~
1106 ~~and track applications;~~

1107 [KI-IAF: 'some effort' is not considered to be an assessable point of conformance and of no value, hence no mapping.]

1108 b) At Level 2:

1109 i) For physical transactions, the Applicant shall identify himself/herself in person by either using
1110 a secret as described above, or by biometric verification (comparing a captured biometric
1111 sample to a reference biometric sample that was enrolled during a prior encounter);

1112 [KI-IAF: AL2_CM_CRD#015]

1113 ii) [KI-IAF: Note that there is no requirement at AL3 which is equivalent to that at AL2 as expressed by §5.3.1.2.11
1114 d) ii), although in all good reason there should be. This void clause is included here for the sake of alignment
1115 between AL2 and AL3 in the mapping with the Kantara SAC.]

- 1116 iii) For electronic transactions, the Applicant shall identify himself/herself in any new transaction
1117 (beyond the first transaction or encounter) by presenting a temporary secret which was
1118 established during a prior transaction or encounter, or sent to the Applicant’s phone number,
1119 email address, or physical address of record.
1120 [*KI-IAF: AL2_CM_CRD#016*]
- 1121 c) At Level 3:
- 1122 i) For physical transactions, the Applicant shall identify himself/herself in person by either using
1123 a secret as described in §5.3.1.6.2 , or through the use of a biometric that was recorded during
1124 a prior encounter. Temporary secrets shall not be reused.
1125 [*KI-IAF: AL3_CM_CRD#015*]
- 1126 ii) If the CSP issues permanent secrets during a physical transaction, then they shall be loaded
1127 locally onto a physical device that is issued in person to the applicant; **when it is not a physical**
1128 **transaction permanent secrets must be**¹⁸ delivered in a manner that confirms the address of
1129 record;
1130 [*KI-IAF: AL3_CM_CRD#017*]
- 1131 iii) For electronic transactions, the Applicant shall identify himself/herself in each new electronic
1132 transaction by presenting a temporary secret which was established during a prior transaction
1133 or encounter, or sent to the Applicant’s phone number, email address, or physical address of
1134 record.
1135 [*KI-IAF: AL3_CM_CRD#016*]
- 1136 iv) Permanent secrets shall only be issued to the applicant within a protected session.
1137 [*KI-IAF: AL3_CM_CRD#018*]
- 1138 d) At Level 4:
- 1139 i) Only physical transactions apply. The Applicant shall identify himself/herself in person in
1140 each new physical transaction through the use of a biometric that was recorded during a prior
1141 encounter.¹⁹
1142 [*KI-IAF: AL4_CM_CRD#015*]
- 1143 ii) If the CSP issues permanent secrets, then they shall be loaded locally onto a physical device
1144 that is issued in person **to the applicant** or delivered in a manner that confirms the address of
1145 record;
1146 [*KI-IAF: AL4_CM_CRD#017*]
- 1147 **5.3.1.5.3** A common reason for breaking up the registration process as described above is to allow the
1148 subscriber to register or obtain tokens for use in two or more environments. This is permissible as long as the
1149 tokens individually meet the appropriate assurance level. However, if the exact number of tokens to be issued
1150 is not agreed upon early in the registration process, then the tokens should be distinguishable so that Verifiers
1151 will be able to detect whether any suspicious activity occurs during the first few uses of a newly issued
1152 token.;
1153 [*KI-IAF: AL4_CM_CRD#017*]
- 1154 [*KI-IAF: The above text is difficult to comprehend (e.g. how does knowing the exact number necessarily mitigate the risk*
1155 *identified?) and might present problems for implementers. At the time of closure of this mapping no advice had been forthcoming*
1156 *from NIST, neither formally or otherwise. Implementors and assessors are advised by the Editor to exercise their own judgement –*
1157 *if risks have been identified, assessed and either accepted at face value or mitigated to an acceptable level, then maybe that*
1158 *works.]*

¹⁸ Added to clarify original NIST text (at least as far as Kantara IAF IAWG best understands it).

¹⁹ Special arrangements can be made for Applicants who are unable to provide the required biometrics.

1159 **5.3.2. Requirements for Educational and Financial Institutions, and other**
1160 **Organizations**

1161 The relationships of many organizations (e.g., corporations, healthcare organizations, educational institutions
1162 and financial institutions) to the individuals who are employees, affiliates, associates, students and customers
1163 are often regulated or supervised by government, while law and regulation place burdens on these
1164 organizations to know the identities of such individuals. The strength of these relationships and the
1165 obligations of organizations to know identities vary considerably, for example employers have legal
1166 obligations to withhold and pay taxes on employees and are regulated by a variety of local, state and Federal
1167 entities, but the certainty enforced in many employment situations is not high. Retail stores are not broadly
1168 required to know their customers, but financial institutions are. Healthcare organizations are regulated at
1169 many levels and are expected to know the identities and professional qualifications of their professional staff,
1170 as are legal and accounting firms. This section identifies several areas where these organizations may
1171 leverage their existing relationships with individuals to act as CAs or CSPs for those individuals and issue
1172 credentials for use with Federal entities.

1173 **5.3.2.1. Employers and Educational Institutions**

1174 *[KI-IAF: This is considered to be specific to NIST SP 800-63-2 Profiling, under 'Current Relationship' or 'Affiliated' Id proofing.]*

1175 At Level 2, employers and educational institutions which elect to become an RA or CSP and issue credentials
1176 to employees or students, shall:

- 1177 a) verify the identity of their employees or students by means comparable to those stated in §5.3.1.2
1178 for Level 2 either in-person by inspection of a corporate- or school-issued picture ID, or through
1179 **online (i.e. remote)** processes;
- 1180 b) effect notification of the credential via the distribution channels normally used for sensitive,
1181 personal communications.

1182 *[KI-IAF: AL2_ID_IDV#010, AL2_ID_CRV#010, AL2_ID_CRV#020, AL2_ID_SCV#010:*
1183 *additionally, see mappings in §5.3.1.2]*

1184 **5.3.2.2. Professional Institutions**

1185 *[KI-IAF: This is considered to be specific to NIST SP 800-63-2 Profiling, under 'Current Relationship' or 'Affiliated' Id proofing.*
1186 *It is recommended that such profiling is mapped against ALn_ID_IDV#010 and ALn_ID_SCV#010 for the applicable Assurance*
1187 *Level, where the cited criteria do not fully encompass the 800-63-2 requirements or the service in question employs alternative*
1188 *means.]*

1189 Federal laws and regulation impose requirements for institutions in certain businesses to confirm the
1190 educational and licensing credentials for selected employees or affiliates. For example, a health care
1191 organization that has accepted the Medicare "Conditions for Participation" is required to examine the
1192 credentials for each candidate for the medical staff.

1193 **5.3.2.2.1** Where such institutions have satisfied these regulatory requirements through a prior in-person
1194 appearance by the candidate, with verification of:

- 1195 a) a current primary Government Picture ID that contains Applicant, picture, and either address of
1196 record or nationality of record (e.g., driver's license or passport);

1197 *[KI-IAF: AL2/3/4_ID_IPV#010+NIST SP 800-63-2 Profiling]*

1198 b) post-secondary education/training of two or more years appropriate for the position (e.g., an
1199 appropriate medical degree); and
1200 [KI-IAF: AL2/3/4_ID_SCV#010 +NIST SP 800-63-2 Profiling]

1201 c) state or federal licensure (e.g., as a physician).
1202 [KI-IAF: AL2/3/4_ID_SCV#010 +NIST SP 800-63-2 Profiling]

1203 [KI-IAF: AL3_ID_IDV#010 +NIST SP 800-63-2 Profiling]

1204 5.3.2.2.2 ... then, that institution may issue e-authentication tokens and credentials to those employees
1205 and affiliates with verified credentials at Levels 2, 3, or 4 provided that

1206 a) the issuance process is either :

1207 i) in-person (mandatory at Level 4); or
1208 [KI-IAF: AL2/3/4_CM_CRD#015 +NIST SP 800-63-2 Profiling]

1209 ii) for Levels 2 and 3, the remote issuance process incorporates the address/phone
1210 number confirmation appropriate for that level,
1211 [KI-IAF: AL2/3_ID_RPV#020 e, f, g)]

1212 and

1213 e) they meet the corresponding provisions of Sections 6 through 9 for that Level.
1214 [KI-IAF: See mappings in §6.3, §7.3, §8.3, §9.3, at the applicable Level]

1215

1216 5.3.2.3. Customer Identification Programs

1217 Federal law, including the Bank Secrecy Act and the USA PATRIOT Act, imposes a duty on financial
1218 institutions to “know their customers” and report suspicious transactions to help prevent money laundering
1219 and terrorist financing. Many financial institutions are regulated by Federal agencies such as the Office of
1220 the Comptroller of the Currency (OCC) or other members of the Federal Financial Institutions Examination
1221 Council (FFIEC) and the Securities and Exchanges Commission (SEC). These regulators normally require
1222 the institutions to implement a Customer Identification Program.

1223 [KI-IAF: This is considered to be specific to NIST SP 800-63-2 Profiling, under ‘Current Relationship’ or ‘Affiliated’ Id proofing.
1224 It is recommended that such profiling is mapped against ALn_ID_CRV#nnn (using whichever criteria best meet the practices of the
1225 CSP), and where the cited criteria do not fully encompass the 800-63-2 requirements or the service in question employs alternative
1226 means, the CSP employs the provisions of SCV#010 for the applicable Assurance Level.]

1227 The following provisions apply to Federally-regulated financial institutions, brokerages and dealers subject to
1228 such Federal regulation that implement such a Customer Identification Program:

1229 [KI-IAF: AL3_ID_IDV#010 +NIST SP 800-63-2 Profiling]

1230 a) At Level 2, such institutions may issue credentials to their customers via the mechanisms
1231 normally used for online banking or brokerage credentials and may use online banking or
1232 brokerage credentials and tokens as Level 2 e-authentication credentials and tokens, provided
1233 they meet the provisions of Sections 6 through 9 for Level 2.
1234 [KI-IAF: AL2_ID_SCV#010 +NIST SP 800-63-2 Profiling. In addition, see mappings in §6.3, §7.3, §8.3, §9.3,
1235 at Level 2.]

1236 b) At Level 3, such institutions may issue credentials to their customers via the mechanisms
1237 normally used for online banking or brokerage credentials and may use online banking or
1238 brokerage credentials and tokens as Level 3 e-authentication credentials and tokens, provided:

1239 i) The customers have been in good standing with the institution for a period of at
1240 least 1 year prior to the issuance of e-authentication credentials, and

- 1241 [KI-IAF: AL3_ID_SCV#010 + NIST SP 800-63-2 Profiling. Kantara has no such requirement.
1242 It is unfortunate that 800-63 offers no further mechanisms which might compensate for the 1 year
1243 requirement if the institution undertook additional measures.]
- 1244 ii) The credentials and tokens meet the provisions of Sections 6 through 9 for Level
1245 3.
1246 [KI-IAF: + NIST SP 800-63-2 Profiling. See mappings in §6.3, §7.3, §8.3, §9.3, at Level 3.]
- 1247 c) At Level 4, such institutions may issue credentials to their customers via the mechanisms
1248 normally used for online banking or brokerage credentials and may use online banking or
1249 brokerage credentials and tokens as Level 4 e-authentication credentials, provided:
- 1250 i) The customers have appeared in-person before a representative of the financial
1251 institution, and the representative has inspected a Government issued primary
1252 Photo-ID and compared the picture to the customer; and
1253 [KI-IAF: AL4_ID_IPV#010, AL4_ID_IPV#030, AL4_ID_IPV#040, AL4_ID_SCV#010 +NIST
1254 SP 800-63-2 Profiling]
- 1255 ii) The credentials and tokens meet all additional provisions of Section 5, as well as
1256 all provisions in Sections 6 through 9 for Level 4, as appropriate.
1257 [KI-IAF: (c) above allows use of ‘normal’ banking mechanisms for issuance: therefore all
1258 provisions (and mappings) of §5.3.4 apply, save those which directly address issuance.
1259 Additionally, see mappings in §6.3, §7.3, §8.3, §9.3, at Level 4.]

1260 **5.3.3. Requirements for Certificates Issued under FPKI and Mapped Policies**

1261 [KI-IAF: This is considered to be specific to NIST SP 800-63-2 Profiling and CSPs exercising their rights under a claim of
1262 compliance with SP 800-63-2 should develop a profile under the above heading, but for the SAC requirements mapped through the
1263 Assurance Level-specific mappings in the respective part of §5.3.1.]

1264 **5.3.3.1** The identity proofing and certificate issuance processes specified in the Federal PKI Certificate
1265 Policies [FBCA1, FBCA2, FBCA3] are considered equivalent to the requirements specified in Section 5.3.1
1266 in accordance with [Appendix B](#).

1267 **5.3.3.1** At Level 2, agencies may rely on any CA whose policy satisfies the identity proofing and
1268 registration requirements specified for Level 2, in addition to any CA cross-certified with the Federal Bridge
1269 CA under one of the certificate policies identified in Appendix B as a Level 2 certificate or a policy mapped
1270 to one of those policies through cross-certificates.

1271 **5.3.3.2** For Levels 3 and 4, agencies shall only accept PKI certificates issued by a CA cross-certified with
1272 the Federal Bridge CA under one of the certificate policies identified in Appendix B as a Level 3 or Level 4
1273 certificate or a policy mapped to one of those policies through cross-certificates.

1274 **5.3.3.3** The identity proofing and certificate issuance processes specified in Federal Information
1275 Processing Standard (FIPS) 201, ‘Personal Identity Verification’ [FIPS201], meet and exceed the Level 4
1276 requirements specified in the preceding section.

1277 **5.3.4. Requirements for One-Time Use**

1278 [KI-IAF: This is not considered to be meaningful within a KI / Federation.]

1279 **5.3.4.1** For infrequently used applications, issuance and maintenance of credentials would be prohibitively
1280 expensive. Claimants can be authenticated for immediate one-time access to an application for Levels 1
1281 through 3.

1282 **5.3.4.2** At Level 1, there is no requirement for identity-proofing before one-time use.

1283 5.3.4.3 At Levels 2 and 3, application owners act as the RA/CSP in the remote registration processes
1284 described in Section 5.3.1, using processes that do not require confirmation of the address of record and
1285 omitting credential issuance.

1286 5.3.4.4 For immediate one-time access at Level 2, application owners can use the registration processes
1287 specified in 5.3.1.2.11 d) vii) 2) & 3) (respectively) that:

1288 a) Confirm "the ability of the Applicant to receive telephone communications or text message
1289 at phone number or e-mail address associated with the Applicant in records"; or

1290 b) Subsequently send a "notice to an address of record confirmed in the records check."

1291 5.3.4.5 For immediate one-time access at Level 3, application owners can use the registration process
1292 specified in 5.3.1.3.11 d) iii) 1) that:

1293 s) Confirms "the ability of the Applicant to receive telephone communications at a phone number
1294 associated with the Applicant in records while recording the Applicant's voice or using alternative
1295 means that establish an equivalent level of non-repudiation."

1296 5.3.5. Requirements for Derived Credentials

1297 *[KI-IAF: Separation has been provided between these clauses and those addressing id proofing per se, because these substitute*
1298 *only for the proof of id but not for the overall credential issuance processes, the requirements for which must still be observed in*
1299 *their respective types and ALs.]*

1300 5.3.5.1 [At all levels] where the Applicant already possesses recognized authentication credentials, the
1301 CSP may choose to identity proof the Claimant by verifying possession and control of the token associated
1302 with the credentials and issue a new derived credential, **subject to the following specific provisions.**

1303 *[KI-IAF: AL1/2/3/4_ID_IDV#000, AL1/2/3/4_ID_IDV#010]*

1304 5.3.5.2 Before issuing any derived credential the CSP shall verify the original credential status and shall
1305 verify that the corresponding token is possessed and controlled by the Claimant.

1306 *[KI-IAF: AL1/2/3/4_ID_IDV#010]*

1307
1308 5.3.5.3 The status of the original credential should be re-checked at a later date (e.g. after a week) to
1309 confirm that it was not compromised at the time of issuance of the derived credential. (This guards against
1310 the case where an Attacker requests the desired credential before revocation information can be updated.)

1311 *[KI-IAF: This clause is recommended but not mandatory, and the SAC have a general practice of being definitive (not absolutely,*
1312 *but as a goal). Hence this clause has NOT been realised as a new SAC criterion since it would force significant load on an issuer,*
1313 *plus become complicated when the issuer was not the verifier.]*

1314 5.3.5.4 In some cases, there may be a desire to tightly-couple the revocation status of the derived
1315 credential to the original. In this case, it is the responsibility of the CSP that issued the derived credential to
1316 ensure that a tight coupling is maintained. For example, the issuer of the derived credential could regularly
1317 monitor the status of the primary credential.^{20 21})

1318 *[KI-IAF: As above.]*

1319 *[KI-IAF: The above paragraph was previously at the end of §5.3.5 but has been placed here because of its relationship to the*
1320 *preceding paragraph and the fact that its original placement had nothing to do with the clauses now following.]*

²⁰ This document does not require or prevent CSPs from linking the expiration of the original and derived credentials. However, where the revocation status is tightly coupled, this may simplify revocation procedures.

²¹ Requirements for derived credentials issued by the same CSP are at the end of Section 5.3.1.

- 1321 5.3.5.5 Further, the CSP shall record the details of the original credential used as the basis for derived
1322 credential issuance.
1323 [KI-IAF: AL2/3/4_ID_IDC#020]
- 1324 5.3.5.6 The CSP may issue a Level 2 derived credential based on proof of possession of a
1325 Level 3 or 4 token. Before issuing the derived credential, the CSP shall:
- 1326 a) For in-person issuance, ensure that the claimant is the Applicant;
1327 [KI-IAF: AL2_ID_IDC#030]
- 1328 b) For remote issuance, either electronically transmitted, or physically shipped
1329 with a token to a claimant, ensure that token activation requires proof of
1330 possession of both the derived token and the original Level 3 or Level 4 token.
1331 [KI-IAF: AL2_ID_IDC#030]
- 1332 5.3.5.7 The CSP may issue a Level 3 derived credential based on proof of possession of a
1333 Level 4 token. Before issuing the derived credential, the CSP shall:
- 1334 a) For in-person issuance, ensure that the claimant is the Applicant;
1335 [KI-IAF: AL3_ID_IDC#030]
- 1336 b) For remote issuance, either electronically transmitted, or physically shipped
1337 with a token to a claimant, ensure that token activation requires proof of
1338 possession of both the derived token and the original Level 4 token.
1339 [KI-IAF: AL3_ID_IDC#030]
- 1340 5.3.5.8 The CSP may issue a derived Level 4 credential for a suitable Level 4 capable token, based on an
1341 original Level 4 credential. Before issuing the derived Level 4 credential **in-person**, the CSP shall:
- 1342 a) obtain and verify a copy of a biometric recorded when the original credential was issued. If
1343 the biometric reference is not available from the Level 4 token (e.g. the signed biometric data
1344 object on a PIV card), it may be obtained from elsewhere, as long as its authenticity is
1345 **established**;
1346 [KI-IAF: AL4_ID_IDC#020]
- 1347 b) compare a fresh biometric sample obtained in-person from the Applicant to the reference
1348 biometric retained from the original Level 4 credential and determine that they match, and;
1349 [KI-IAF: AL4_ID_IDC#030]
- 1350 c) determine that the token that contains the token secret associated with the derived credential
1351 meets the requirements of Table 6-4.
- 1352 5.3.5.9 If the derived credential is revoked, the CSP that issued the derived credential may notify the
1353 issuer of the original credential, if the reason for revocation might motivate action by the issuer of the
1354 original credential and applicable law, regulation, and agreements permit such notification.
1355 [KI-IAF: As 5.3.5.3 above.]
- 1356
1357

1358 6. Tokens

1359 The concept of a token was introduced in Section 4. This section provides a more in-depth treatment of e-
1360 authentication tokens. Section 6.1 describes classes of tokens recognized by this recommendation and how
1361 they can be combined in practice. Section 6.2 identifies threats and mitigation strategies applicable to tokens.
1362 Section 6.3 maps recognized classes of tokens to assurance levels and identifies any required threat
1363 mitigation strategies.

1364 6.1. Overview

1365 In the e-authentication context, a token contains a secret to be used in authentication processes. Tokens are
1366 possessed by a Claimant and controlled through one or more of the traditional authentication factors
1367 (*something you know, have, or are*). Figure 2 depicts an abstract model for a token.

1368 The outer box shown in Figure 2 is the token. Tokens may exist in hardware (e.g., a smart card), software
1369 (e.g., a software cryptographic module), or may only exist in human memory. The inner box represents the
1370 token secret that is stored within the token. The output of a token is the *token authenticator*, which is the
1371 value that is provided to the protocol stack for transmission to the Verifier to prove that the Claimant
1372 possesses and controls the token. The token authenticator may be the token secret, or a transformation of the
1373 token secret.

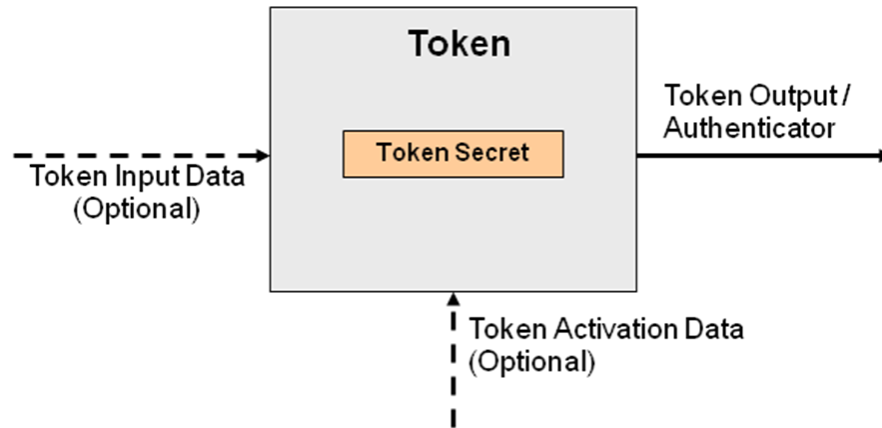
1374 There are two optional inputs to the token: *token input data*; and *token activation data*. Token input data,
1375 such as a challenge or nonce, may be required to generate the token authenticator. Token input data may be
1376 supplied by the user or be a feature of the token itself (e.g. the clock in an OTP device). Token activation
1377 data, such as a PIN or biometric, may be required to activate the token and permit generation of an
1378 authenticator. Token activation data is needed when a Claimant controls the token through *something you*
1379 *know* or *something you are*. (Where the token is something you know, such as a password or memorized
1380 secret, token activation is implicit.)

1381 The *authenticator* is generated through the use of the token. In the general case, an authenticator is generated
1382 by performing a mathematical function using the token secret and one or more optional token input values (a
1383 nonce or challenge):

1384
1385
$$\text{Authenticator} = \text{Function} (\text{<token secret>} [, \text{<nonce>}] [, \text{<challenge>}])$$

1386
1387 As noted above, in the trivial case, the authenticator may be the token secret itself (e.g., where the token is a
1388 password).

1389



1390
1391
1392
1393

Figure 2 - *Token Model*

1394 **6.1.1. Single-factor versus Multi-factor Tokens**

1395 Tokens are characterized by the number and types of authentication factors that they use. (See Section 4.3 for
1396 discussion on three types of authentication factors.) For example, a password is something you know, a
1397 biometric is something you are, and a cryptographic identification device is something you have. Tokens may
1398 be single-factor or multi-factor tokens as described below:

- 1399 a) *Single-factor Token* – A token that uses one of the three factors to achieve authentication. For
1400 example, a password is *something you know*. There are no additional factors required to
1401 activate the token, so this is considered single factor.
- 1402 b) *Multi-factor Token* – A token that uses two or more factors to achieve authentication. For
1403 example, a private key on a smart card that is activated via PIN is a multi-factor token. The
1404 smart card is *something you have*, and *something you know* (the PIN) is required to activate
1405 the token.

1406 This document does not differentiate between tokens that require two factors and three factors, as two factors
1407 are sufficient to achieve the highest level recognized in this document. Other applications or environments
1408 may require such a differentiation.

1409 **6.1.2. Token Types**

1410 These guidelines recognize the following types of tokens for e-authentication.

- 1411 a) *Memorized Secret Token* – A secret shared between the Subscriber and the CSP. Memorized
1412 Secret Tokens are typically character strings (e.g., passwords and passphrases) or numerical
1413 strings (e.g., PINs.) The token authenticator presented to the Verifier in an authentication
1414 process is the secret itself (e.g. the password or passphrase itself). Memorized secret tokens
1415 are *something you know*.
- 1416 b) *Pre-registered Knowledge Token* – A series of responses to a set of prompts or challenges.
1417 These responses may be thought of as a set of shared secrets. The set of prompts and
1418 responses are established by the Subscriber and CSP during the registration process. The
1419 token authenticator is the set of memorized responses to pre-registered prompts during a
1420 single run of the authentication process. An example of a Pre-registered Knowledge Token
1421 would be establishing responses for prompts such as “What was your first pet’s name?”
1422 During the authentication process, the Claimant is asked to provide the appropriate responses

- 1423 to a subset of the prompts. Alternatively, a Subscriber might select and memorize an image
1424 during the registration process. In an authentication process, the Claimant is prompted to
1425 identify the correct images from a set(s) of similar images. Transactions from previously
1426 authenticated sessions could be accepted as Pre-registered Knowledge Tokens. Pre-registered
1427 Knowledge Tokens are *something you know*.
- 1428 c) *Look-up Secret Token* – A physical or electronic token that stores a set of secrets shared
1429 between the Claimant and the CSP. The Claimant uses the token to look up the appropriate
1430 secret(s) needed to respond to a prompt from the Verifier (the token input). For example, a
1431 Claimant may be asked by the Verifier to provide a specific subset of the numeric or character
1432 strings printed on a card in table format. The token authenticator is the secret(s) identified by
1433 the prompt. Look-up secret tokens are *something you have*.
- 1434 d) *Out of Band Token* – A physical token that is uniquely addressable and can receive a Verifier-
1435 selected secret for one-time use. The device is possessed and controlled by the Claimant and
1436 supports private communication²² over a channel that is separate from the primary channel for
1437 e-authentication. The token authenticator is the received secret and is presented to the Verifier
1438 using the primary channel for e-authentication. For example, a Claimant attempts to log into a
1439 website and receives a text message on his or her cellular phone, PDA, pager, or land line
1440 (pre-registered with the CSP during the registration phase) with a random authenticator to be
1441 presented as a part of the electronic authentication protocol. Out of Band Tokens are
1442 *something you have*.
- 1443 e) *Single-factor (SF) One-Time Password (OTP) Device* – A hardware device that supports the
1444 spontaneous generation of one-time passwords. This device has an embedded secret that is
1445 used as the seed for generation of one-time passwords and does not require activation through
1446 a second factor. Authentication is accomplished by providing an acceptable one-time
1447 password and thereby proving possession and control of the device. The token authenticator
1448 is the one-time password. For example, a one-time password device may display 6 characters
1449 at a time. SF OTP devices are *something you have*.
- 1450 f) *Single-factor (SF) Cryptographic Device* – a hardware device that performs cryptographic
1451 operations on input provided to the device. This device does not require activation through a
1452 second factor of authentication. This device uses embedded symmetric or asymmetric
1453 cryptographic keys. Authentication is accomplished by proving possession of the device. The
1454 token authenticator is highly dependent on the specific cryptographic device and protocol, but
1455 it is generally some type of signed message. For example, in TLS, there is a “certificate
1456 verify” message. SF Cryptographic Devices are *something you have*.
- 1457 g) *Multi-factor (MF) Software Cryptographic Token* – A cryptographic key is stored on disk or
1458 some other “soft” media and requires activation through a second factor of authentication.
1459 Authentication is accomplished by proving possession and control of the key. The token
1460 authenticator is highly dependent on the specific cryptographic protocol, but it is generally
1461 some type of signed message. For example, in TLS, there is a “certificate verify” message.
1462 The MF software cryptographic token is *something you have*, and it may be activated by either
1463 *something you know* or *something you are*.
- 1464 h) *Multi-factor (MF) One-Time Password (OTP) Device* – A hardware device that generates one-
1465 time passwords for use in authentication and which requires activation through a second factor
1466 of authentication. The second factor of authentication may be achieved through some kind of
1467 integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface

²² Private communication means the Verifier’s message is sent directly to the Claimant’s device.

1468 (e.g., USB port). The one-time password is typically displayed on the device and manually
1469 input to the Verifier as a password, although direct electronic input from the device to a
1470 computer is also allowed. The token authenticator is the one-time password. For example, a
1471 one-time password device may display 6 characters at a time. The MF OTP device is
1472 *something you have*, and it may be activated by either *something you know* or *something you*
1473 *are*.

1474 i) *Multi-factor (MF) Cryptographic Device* – A hardware device that contains a protected
1475 cryptographic key that requires activation through a second authentication factor.
1476 Authentication is accomplished by proving possession of the device and control of the key.
1477 The token authenticator is highly dependent on the specific cryptographic device and protocol,
1478 but it is generally some type of signed message. For example, in TLS, there is a “certificate
1479 verify” message. The MF Cryptographic device is *something you have*, and it may be
1480 activated by either *something you know* or *something you are*.

1481

1482 **6.1.3. Token Usage**

1483 An authentication process may involve a single token, or a combination of two or more tokens, as described
1484 below.

1485 a) *Single-token authentication* – The Claimant presents a single token authenticator to prove his
1486 or her identity to the Verifier. For example, when a Claimant attempts to log into a password
1487 protected website, the Claimant enters a username and password. In this instance, only the
1488 password would be considered to be a token.

1489 b) *Multi-token authentication* – The Claimant presents token authenticators generated by two or
1490 more tokens to prove his or her identity to the Verifier. The combination of tokens is
1491 characterized by the combination of factors used by the tokens (both inherent in the
1492 manifestation of the tokens, and those used to activate the tokens). A Verifier that requires a
1493 Claimant to enter a password and use a single-factor cryptographic device is an example of
1494 multi-token authentication. The combination is considered multi-factor, since the password is
1495 *something you know* and the cryptographic device is *something you have*.

1496 **6.1.4. Multi-Stage Authentication Using Tokens**

1497 Multi-stage authentication processes, which use a single-factor token to obtain a second token, do not
1498 constitute multi-factor authentication. The level of assurance associated with the compound solution is the
1499 assurance level of the weakest token.

1500 For example, some cryptographic mobility solutions allow full or partial cryptographic keys to be stored on
1501 an online server and downloaded to the Claimant’s local system after successful authentication using a
1502 password or passphrase. Subsequently, the Claimant can use the downloaded software cryptographic token to
1503 authenticate to a remote Verifier for e-authentication. This type of solution is considered only as strong as the
1504 password provided by the Claimant to obtain the cryptographic token.

1505 **6.1.5. Assurance Level Escalation**

1506 In certain circumstances, it may be desirable to raise the assurance level of an e-authentication session
1507 between a Subscriber and an RP in the middle of the application session. This guideline recognizes a special
1508 case of multi-token authentication, where a primary token is used to establish a secure session, and a

1509 secondary token is used later in the session to present a second token authenticator. Even though the two
 1510 tokens were not used at the same time, this document recognizes the result as a multi-token authentication
 1511 scheme (which may upgrade the overall level of assurance). In these authentication scenarios, the level of
 1512 assurance achieved by the two stages in combination is the same as a multi-token authentication scheme
 1513 using the same set of tokens. Table 7 describes the highest level of assurance achievable through a
 1514 combination of two token types.

1515 **6.2. Token Threats**

1516 An Attacker who can gain control of a token will be able to masquerade as the token’s owner. Threats to
 1517 tokens can be categorized based on attacks on the types of authentication factors that comprise the token:

- 1518 a) *Something you have* may be lost, damaged, stolen from the owner or cloned by the Attacker.
 1519 For example, an Attacker who gains access to the owner’s computer might copy a software
 1520 token. A hardware token might be stolen, tampered with, or duplicated.
- 1521 b) *Something you know* may be disclosed to an Attacker. The Attacker might guess a password
 1522 or PIN. Where the token is a shared secret, the Attacker could gain access to the CSP or
 1523 Verifier and obtain the secret value. An Attacker may observe the entry of a PIN or passcode,
 1524 find a written record or journal entry of a PIN or passcode, or may install malicious software
 1525 (e.g., a keyboard logger) to capture the secret. Additionally, an Attacker may determine the
 1526 secret through off-line attacks on network traffic from an authentication attempt. Finally, an
 1527 Attacker may be able to gain information about a Subscriber’s Pre-registered Knowledge
 1528 researching the subscriber or through other social engineering techniques. (For example, the
 1529 subscriber might refer to his or her first pet in a conversation or blog.)
- 1530 c) *Something you are* may be replicated. An Attacker may obtain a copy of the token owner’s
 1531 fingerprint and construct a replica - assuming that the biometric system(s) employed do not
 1532 block such attacks by employing robust liveness detection techniques.

1533 This document assumes that the Subscriber is not colluding with the Attacker who is attempting to falsely
 1534 authenticate to the Verifier. With this assumption in mind, the threats to the token(s) used for e-
 1535 authentication are listed in Table 4, along with some examples.
 1536
 1537
 1538

Table 4 – Token Threats

Token Threats/Attacks	Description	Examples
Theft	A physical token is stolen by an Attacker.	A hardware cryptographic device is stolen.
		A One-Time Password device is stolen.
		A look-up secret token is stolen.
		A cell phone is stolen.
Discovery	The responses to token prompts are easily discovered through searching various data sources.	The question “What high school did you attend?” is asked as a Pre-registered Knowledge Token, when the answer is commonly found on social media websites.
Duplication	The Subscriber’s token has been copied with or without his or her knowledge.	Passwords written on paper are disclosed.
		Passwords stored in an electronic file are copied.
		Software PKI token (private key) copied.
		Look-up token copied.
Eavesdropping	The token secret or authenticator is revealed to the Attacker as the Subscriber is submitting the token to send over the network.	Passwords are learned by watching keyboard entry.
		Passwords are learned by keystroke logging software.
		A PIN is captured from PIN pad device.

Offline cracking	The token is exposed using analytical methods outside the authentication mechanism.	A key is extracted by differential power analysis on stolen hardware cryptographic token.
		A software PKI token is subjected to dictionary attack to identify the correct password to use to decrypt the private key.
Phishing or pharming	The token secret or authenticator is captured by fooling the Subscriber into thinking the Attacker is a Verifier or RP.	A password is revealed by Subscriber to a website impersonating the Verifier.
		A password is revealed by a bank Subscriber in response to an email inquiry from a Phisher pretending to represent the bank.
		A password is revealed by the Subscriber at a bogus Verifier website reached through DNS re-routing.
Social engineering	The Attacker establishes a level of trust with a Subscriber in order to convince the Subscriber to reveal his or her token or token secret.	A password is revealed by the Subscriber to an officemate asking for the password on behalf of the Subscriber's boss.
		A password is revealed by a Subscriber in a telephone inquiry from an Attacker masquerading as a system administrator.
Online guessing	The Attacker connects to the Verifier online and attempts to guess a valid token authenticator in the context of that Verifier.	Online dictionary attacks are used to guess passwords.
		Online guessing is used to guess token authenticators for a one-time password token registered to a legitimate Claimant.

1539

1540 **6.2.1. Threat Mitigation Strategies**

1541 Token related mechanisms that assist in mitigating the threats identified above are summarized in Table 5.

1542

1543

Table 5 - Mitigating Token Threats

Token Threat/Attack	Threat Mitigation Mechanisms
Theft	- Use multi-factor tokens which need to be activated through a PIN or biometric.
Duplication	- Use tokens that are difficult to duplicate, such as hardware cryptographic tokens.
Discovery	- Use methods in which the responses to prompts cannot be easily discovered.
Eavesdropping	- Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator. - Use tokens that generate authenticators based on a token input value. - Establish tokens through a separate channel.
Offline cracking	- Use a token with a high entropy token secret - Use a token that locks up after a number of repeated failed activation attempts.
Phishing or pharming	- Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator.
Social engineering	- Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator.
Online guessing	- Use tokens that generate high entropy authenticators.

1544

1545 There are several other strategies that may be applied to mitigate the threats described in Table 5:

1546

- 1547 a) *Multiple factors* make successful attacks more difficult to accomplish. If an Attacker needs to
1548 steal a cryptographic token and guess a password, then the work to discover both factors may
1549 be too high.
- 1550 b) *Physical security mechanisms* may be employed to protect a stolen token from duplication.
1551 Physical security mechanisms can provide tamper evidence, detection, and response.
- 1552 c) *Imposing password complexity rules* may reduce the likelihood of a successful guessing
1553 attack. Requiring the use of long passwords that don't appear in common dictionaries may
1554 force Attackers to try every possible password.
- 1555 d) *System and network security controls* may be employed to prevent an Attacker from gaining
1556 access to a system or installing malicious software.
- 1557 e) *Periodic training* may be performed to ensure the Subscriber understands when and how to
1558 report compromise (or suspicion of compromise) or otherwise recognize patterns of behavior
1559 that may signify an Attacker attempting to compromise the token.
- 1560 f) *Out of band techniques* may be employed to verify proof of possession of registered devices
1561 (e.g., cell phones).

1562

1563 **6.3. Token Assurance Levels**

1564 This section discusses the requirements for tokens used at various levels of assurance.

1565 **6.3.1. Requirements per Assurance Level**

1566 The following sections list token requirements for single and multi-token authentication.

1567 **6.3.1.1. Single Token Authentication**

1568 The following tables list the assurance levels that may be achieved by each of the token types when used in a
1569 single-token authentication scheme. For each assurance level the requirements for each token are described
1570 as are the requirements for verification of that token type. If token requirements are listed only at one
1571 assurance level, the token may be used at lower levels but shall satisfy the requirements given at whatever
1572 level is listed. If there is more than one box under "Verifier Requirements" for a given token type, it is only
1573 necessary to satisfy the requirements in one box.
1574

1575 [KI-IAF: The following tables have been re-structured from their 'all-in-one' format in the original NIST publication, with the
 1576 intention of dealing with each AL discretely. References have been added for the purpose of uniquely identifying each clause but
 1577 their sequence has no other intention or meaning.]

1578 Table 6-1 - Token Requirements for Assurance Level 1

Token Requirements	Verifier Requirements
6.3.1.1.1 Memorized Secret Token	
<p>a) The memorized secret may be a user chosen string consisting of 6 or more characters chosen from an alphabet of 90 or more characters, a randomly generated PIN consisting of 4 or more digits, or a secret with equivalent entropy.²³ [KI-IAF: by reference to Table A.1, the minimum entropy this can produce is 13.3 bits (random 4-digit pin).] [KI-IAF: AL1_CM_CTR#020 a), AL1_CM_CRN#040 a)]</p> <p>b) CSP implements dictionary or composition rule to constrain user-generated secret [KI-IAF: AL1_CM_CTR#020 a), AL1_CM_CRN#040 a)]</p>	<p>c) The Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period. [KI-IAF: AL1_CM_ASS#035]</p> <p>Note: While an implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See Section 8.2.3 for more detailed advice.</p>
6.3.1.1.2 Pre-Registered Knowledge Token	
<p>a) The secret provides at least 14 bits of entropy.²³ [KI-IAF: AL1_CM_CTR#020 a), AL1_CM_CRN#040 b) i)]</p>	<p>b) The Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period. [KI-IAF: AL1_CM_ASS#035]</p> <p>Note: While an implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See Section 8.2.3 for more detailed advice.</p>
<p>c) The entropy in the secret cannot be directly calculated, e.g., user chosen or personal knowledge questions. [KI-IAF: AL1_CM_CTR#020 a), AL1_CM_CRN#040 b) ii)]</p> <p>d) If the questions are not supplied by the user, the user shall select prompts from a set of at least five questions. [KI-IAF: AL1_CM_CTR#020 a), AL1_CM_CRN#040 b) iii)]</p>	<p>e) For these purposes, an empty answer is prohibited. [KI-IAF: AL1_CM_CRN#040 b) ii & iii]</p> <p>f) The Verifier shall verify the answers provided for at least three questions, and shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period. [KI-IAF: AL1_CM_ASS#035]</p> <p>Note: While an implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See Section 8.2.3 for more detailed advice.</p>

1579

1580 Table 6-2 - Token Requirements for Assurance Level 2

Token Requirements	Verifier Requirements
6.3.1.2.1 Memorized Secret Token	
<p>a) The memorized secret may be a randomly generated PIN consisting of 6 or more digits, a user generated string consisting of 8 or more characters chosen</p>	<p>c) The Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period. [KI-IAF: AL2_CM_ASS#035]</p>

²³ For more information, see Table A.1 in Appendix A.

Token Requirements	Verifier Requirements
<p>from an alphabet of 90 or more characters, or a secret with equivalent entropy.²³ [KI-IAF: AL2_CM_CTR#020 a), AL2_CM_CRN#040 a), '#050]</p> <p>b) CSP implements dictionary or composition rule to constrain user-generated secrets. [KI-IAF: The above clause requires at least 8 bits of entropy; this requires at least 24 (the 'or' allows Kantara to wriggle away from 30)] [KI-IAF: AL2_CM_CTR#020 a), AL2_CM_CRN#040 a), AL2_CM_CRN #050]</p>	<p>Note: While an implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See Section 8.2.3 for more detailed advice.</p>
<p>6.3.1.2.2 Pre-Registered Knowledge Token</p>	
<p>a) The secret provides at least 20 bits of entropy.²³ [KI-IAF: AL2_CM_CTR#020 a), AL2_CM_CRN#040 b) i), AL2_CM_CRN #050]</p>	<p>b) The Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period. [KI-IAF: AL2_CM_ASS#035]</p> <p>Note: While an implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See Section 8.2.3 for more detailed advice.</p>
<p>c) The entropy in the secret cannot be directly calculated, e.g., user chosen or personal knowledge questions. [KI-IAF: AL2_CM_CTR#020 a), AL2_CM_CRN#040 b) ii), AL2_CM_CRN #050]</p> <p>d) If the questions are not supplied by the user, the user shall select prompts from a set of at least seven questions. [KI-IAF: AL2_CM_CTR#020 a), AL2_CM_CRN#040 b) iii), AL2_CM_CRN #050]</p>	<p>e) For these purposes, an empty answer is prohibited. [KI-IAF: AL2_CM_CRN#040 b) ii & iii] – Note: this control needs to be applied at the time that the questions are established, not simply by the Verifier.</p> <p>f) The Verifier shall verify the answers provided for at least five questions, and shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period. [KI-IAF: AL2_CM_ASS#035]</p> <p>Note: While an implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See Section 8.2.3 for more detailed advice.</p>
<p>6.3.1.2.3 Look-up Secret Token</p>	
<p>a) The token authenticator has 64 bits of entropy.²³ [KI-IAF: AL2_CM_CRN#040 c) +NIST SP 800-63-2 Profiling (as a special instance of the requirement below)]</p>	<p>b) N/A [KI-IAF: AL2_CM_ASS#035]</p>
<p>c) The token authenticator has at least 20 bits of entropy.²³ [KI-IAF: AL2_CM_CRN#040 c)]</p>	<p>d) The Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period. [KI-IAF: AL2_CM_ASS#035]</p> <p>Note: While an implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See Section 8.2.3 for more detailed advice.</p>
<p>6.3.1.2.4 Out of Band Token</p>	
<p>a) The token is uniquely addressable and supports communication over a channel that is separate from the primary channel for e-authentication. [KI-IAF: AL2_CM_CRN#040 d)]</p>	<p>b) The Verifier generated secret shall have at least 64 bits of entropy²³ OR [KI-IAF: AL2_CM_AGC#010+NIST SP 800-63-2 Profiling]</p> <p>c) The Verifier-generated secret shall have at least 20 bits of entropy²³ and [KI-IAF: AL2_CM_AGC#010+NIST SP 800-63-2 Profiling]</p> <p>d) The Verifier shall implement a throttling mechanism that effectively limits the number of failed authentication attempts an Attacker can make on the Subscriber's account to 100 or fewer in any 30-day period.</p>

Token Requirements	Verifier Requirements
	<p>[KI-IAF: AL2_CM_ASS#035+NIST SP 800-63-2 Profiling]</p> <p>Note: While an implementation that simply counted all failed authentication attempts in each calendar month and locked out the account when the limit was exceeded would technically meet the requirement, this is a poor choice for reasons of system availability. See Section 8.2.3 for more detailed advice.</p>
6.3.1.2.5 SF One-Time Password Device	
<p>a) Shall use Approved block cipher or hash function to combine a symmetric key stored on device with a nonce to generate a one-time password. [KI-IAF: AL2_CM_CRN#040 e)]</p> <p>b) The nonce may be a date and time, or a counter generated on the device. [KI-IAF: AL2_CM_CRN#040 e)]</p>	<p>c) The one-time password shall have a limited lifetime, on the order of minutes. [KI-IAF: AL2_CM_CRN#055]</p> <p>d) The cryptographic module performing the verifier function shall be validated at FIPS 140-2 Level 1 or higher.²⁴ [KI-IAF: AL2_CM_CRN#070]</p>
6.3.1.2.6 SF Cryptographic Device	
<p>a) The cryptographic module shall be validated at FIPS 140-2 Level 1 or higher.²⁴ [KI-IAF: AL2_CM_CRN#040 f), AL2_CM_CRN#060]</p>	<p>b) Verifier generated token input (e.g., a nonce or challenge) has at least 64 bits of entropy.²³ [KI-IAF: AL2_CM_AGC#010+NIST SP 800-63-2 Profiling]</p>

1581

1582

Table 6-3 - Token Requirements for Assurance Level 3

Token Requirements	Verifier Requirements
6.3.1.3.1 MF Software Cryptographic Token	
<p>a) The cryptographic module shall be validated at FIPS 140-2 Level 1 or higher.²⁴ Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication. [KI-IAF: AL3_CM_CRN#060]</p>	<p>b) Verifier generated token input (e.g., a nonce or challenge) has at least 64 bits of entropy.²³ [KI-IAF: AL3_CM_AGC#010+NIST SP 800-63-2 Profiling]</p>

1583

1584

Table 6-4 - Token Requirements for Assurance Level 4

Token Requirements	Verifier Requirements
6.3.1.4.1 MF OTP Hardware Token	
<p>a) Cryptographic module shall be FIPS 140-2 validated Level 2 or higher; with physical security at FIPS 140-2 Level 3 or higher.²⁴</p> <p>b) The one-time password shall be generated by using an Approved block cipher or hash function to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password.</p> <p>c) The nonce may be a date and time; or a counter generated on</p>	<p>e) The one-time password shall have a limited lifetime of less than 2 minutes. [KI-IAF: AL4_CM_AGC#020]</p>

²⁴ Products validated under subsequent versions of FIPS 140-2 are also acceptable.

Token Requirements	Verifier Requirements
the device. d) Each authentication shall require entry of a password or other activation data through an integrated input mechanism. <i>[KI-IAF: AL4_CM_CRN#070 +NIST SP 800-63-2 Profiling (for all above sub-clauses)]</i>	
6.3.1.4.2 MF Hardware Cryptographic Token	
a) Cryptographic module shall be FIPS 140-2 validated, Level 2 or higher; b) with physical security at FIPS 140-2 Level 3 or higher. ²⁴ c) Shall require the entry of a password, PIN, or biometric to activate the authentication key. d) Shall not allow the export of authentication keys. <i>[KI-IAF: AL4_CM_CRN#075 +NIST SP 800-63-2 Profiling (for all above sub-clauses)]</i>	e) Verifier generated token input (e.g., a nonce or challenge) has at least 64 bits of entropy. ²³ <i>[KI-IAF: AL4_CM_AGC#010+NIST SP 800-63-2 Profiling]</i>

1585

1586 6.3.1.2. Multi-Token Authentication

1587 When two of the token types are combined for a multi-token authentication scheme, Table 7 shows the highest possible assurance level that can
 1588 be achieved by the combination.²⁵

1589

1590

Table 7 - Assurance Levels for Multi-Token E-Authentication Schemes²⁶

	MF Cryptographic Device	MF OTP Device	MF Software Cryptographic Token	SF Cryptographic Device	SF OTP Device	Out of Band Token	Look-up Secret Token	Pre-registered Knowledge Token	Memorized Secret Token
Memorized Secret Token	Level 4	Level 4	Level 3	Level 3	Level 3	Level 3	Level 3	Level 2	Level 2
Pre-registered Knowledge Token	Level 4	Level 4	Level 3	Level 3	Level 3	Level 3	Level 3	Level 2	
Look-up Secret Token	Level 4	Level 4	Level 3	Level 2	Level 2	Level 2	Level 2		
Out of Band Token	Level 4	Level 4	Level 3	Level 2	Level 2	Level 2			
SF OTP Device	Level 4	Level 4	Level 3	Level 2	Level 2				
SF Cryptographic Device	Level 4	Level 4	Level 3	Level 2					
MF Software Cryptographic Token	Level 4	Level 4	Level 3						
MF OTP Device	Level 4	Level 4							
MF Cryptographic Device	Level 4								

1591

1592

[KI-IAF: AL2/3/4_CM_MFA#010+NIST SP 800-63-2 Profiling]

²⁵ Note that the table displays tokens that exhibit the properties of “something you have” and “something you know”.

²⁶ [KI-IAF: redundant entries removed and colour-coding added to give the array enhanced impact.]

1593 The principles used in generating Table 7 are as follows. Level 3 can be achieved using two tokens rated at
1594 Level 2 that represent two different factors of authentication. Since this specification does not address the use
1595 of biometrics as a stand-alone token for remote authentication, achieving Level 3 with separate Level 2
1596 tokens implies *something you have* and *something you know*:

1597 Token (Level 2, *something you have*) + Token (Level 2, *something you know*) → Token(Level 3)

1598 In all other cases, combinations of tokens are considered to achieve the Level of the highest-rated token.

1599 For example, a Memorized Secret Token combined with a Look-up Secret Token can be used to achieve
1600 Level 3 authentication, since the look-up secret token is “something you have” and the Memorized Secret
1601 Token is “something you know”. However, combining a MF software cryptographic token (which is rated at
1602 Level 3) and a Memorized Secret Token (which is rated at Level 2) achieves an overall level of 3, since the
1603 addition of the Memorized Secret Token does not increase the assurance of the combination.

1604 It should be noted that to achieve Level 4 with a single token or token combination, one of the tokens needs
1605 to be usable with an authentication process that strongly resists man-in-the-middle attacks. While it is
1606 possible to meet this requirement with a wide variety of token types, certain choices of tokens may
1607 complicate the task of designing a protocol that meets Level 4 requirements for authentication process (as
1608 described in Section 8 of this document). In particular, one-time password devices that rely exclusively on
1609 the human user for input and output may be especially problematic and may need to be supplemented with a
1610 software cryptographic token to provide strong man-in-the-middle resistance.

1611

1612 7. Token and Credential Management

1613 7.1. Overview

1614 As introduced in Section 4, credentials are objects that bind identity to a token. To maintain the level of
1615 assurance provided by an e-authentication solution, credentials and tokens shall be managed to reflect any
1616 changes in that binding. This section discusses token and credential management activities performed by the
1617 CSP subsequent to the registration, identity proofing and issuance activities described in Section 5. This
1618 includes the lifecycle management activities for the token and credential. The activities that must be
1619 performed by the CSP depend in part upon the nature of the credentials and the tokens themselves~~itself~~.

1620 7.1.1. Categorizing Credentials

1621 This specification categorizes credentials according to two orthogonal perspectives. Some classes of
1622 credentials can be distributed to relying parties, while others cannot be disclosed by the CSP without
1623 compromising the token itself. Another classification indicates whether the binding represented in the
1624 credential is tamper-evident.

1625 Credentials that describe the binding in a way that does not compromise the token are referred to as *Public*
1626 *Credentials*. The classic example of a Public Credential is a public key certificate; it is mathematically
1627 infeasible to calculate the user's private key even with knowledge of the corresponding public key.
1628 Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the token
1629 are considered *Private Credentials*. The classic example of a Private Credential is the hashed value of a
1630 password, since this hash can be used to perform an offline attack on the password.

1631 Credentials that describe the binding between a user and token in a tamper-evident fashion are considered
1632 *Strongly Bound Credentials*. For example, modification of a digitally signed credential (such as a public key
1633 certificate) can be easily detected through signature verification. The binding between a user and token can
1634 be modified in *Weakly Bound Credentials* without invalidating the credentials. Weakly bound credentials
1635 require supplemental integrity protection and/or access controls to ensure that the binding represented by the
1636 credential remains accurate. For example, replacing the value of a hashed password in a password file
1637 associates the user with a new password, so access to this file is restricted to system users and processes.

1638 Strongly bound credential mechanisms require little or no additional integrity protection, whereas weakly
1639 bound credentials require additional integrity protection or access controls to ensure that unauthorized parties
1640 cannot spoof or tamper with the binding of the identity to the token representation within the credential.

1641 Unencrypted password files are private credentials that are weakly bound, and hence need to be afforded
1642 confidentiality as well as integrity protection. Signed password files are private credentials that are strongly
1643 bound and therefore require confidentiality protection but no additional integrity protection. An unsigned
1644 pairing of a public key and the name of its owner or a self-signed certificate is an example of a public
1645 credential that is weakly bound. Finally, a CA-signed public key certificate represents a public credential that
1646 is strongly bound.

1647 CSPs and Verifiers are trusted to obey the requirements in this section as well as Section 8.

1648 7.1.2. Token and Credential Management Activities

1649 The CSP manages tokens and credentials. The RA establishes the Applicant's identity, and the CSP is
1650 responsible for generating credentials and supplying the Subscriber with a token or allowing the Subscriber

1651 to register his or her own token as described in Section 5. The CSP is responsible for some or all of the
1652 following token and credential management activities following issuance of the token and credential:

- 1653 a) *Credential storage* – After the credential has been created, the CSP may be responsible for
1654 maintaining the credentials in storage. In cases where the credentials are stored by the CSP,
1655 the level of security afforded to the credential will depend on the type of credential issued. For
1656 private credentials, additional confidentiality mechanisms are required in storage, whereas for
1657 public credentials, this is not necessary. Similarly, for weakly bound credentials, additional
1658 integrity protection is needed in storage, unlike strongly bound credentials. Finally, credentials
1659 need to be available to allow CSPs and Verifiers to determine the identity of the
1660 corresponding token owner.
- 1661 b) *Token and credential verification services* – In many e-authentication scenarios, the Verifier
1662 and the CSP are not part of the same entity. In these cases, the CSP is responsible for
1663 providing the Verifier with the information needed to facilitate the token and credential
1664 verification process. The CSP may provide token and credential verification services to
1665 Verifiers. For example, the Verifier may request the CSP to verify the password submitted by
1666 the Claimant against the CSP’s local password database.
- 1667 c) *Token and credential renewal /re-issuance* – Certain types of tokens and credentials may
1668 support the process of renewal or re-issuance. During renewal, the usage or validity period of
1669 the token and credential is extended without changing the Subscriber’s identity or token.
1670 During re-issuance, a new credential is created for a Subscriber with a new identity and/or a
1671 new token.

1672 The CSP establishes suitable policies for renewal and re-issuance of tokens and credentials. The
1673 CSP may establish a time period prior to the expiration of the credential, when the Subscriber can
1674 request renewal or re-issuance following successful authentication using his or her existing,
1675 unexpired token and credential. For example, a CSP may allow a digital certificate to be renewed
1676 for another year prior to the expiry of the current certificate by proving possession and control of
1677 the existing token (i.e., the private key).

1678 Once the Subscriber’s credentials have expired, the Subscriber may be required to re-establish his
1679 or her identity with the CSP; this is typically the case with CSPs that issue digital certificates.
1680 Conversely, the CSP may establish a grace period for the renewal or re-issuance of an expired
1681 credential, such that the Subscriber can request renewal/re-issuance of his or her credential even
1682 after it has expired without the need to re-establish his or her identity with the CSP. For example,
1683 if a Claimant attempts to login to a username/password based system on which his or her
1684 password has already expired, and the system supports a grace period, the user may be prompted
1685 to create a new password and supply the last password for verification purposes. The use of
1686 expired tokens or credentials to invoke renewal/re-issuance is more practical when the Verifier
1687 and CSP are part of the same entity.

1688 The public key certificate for a Subscriber may be renewed with the same public key, or may be
1689 re-issued with a new public key. Passwords are seldom renewed so that the life of the existing
1690 password is extended for another period. Usually the account name/password credential for a
1691 Subscriber is renewed by having the Subscriber select a new password.

- 1692 d) *Token and credential revocation and destruction* – The CSP is responsible for maintaining the
1693 revocation status of credentials and destroying the credential at the end of its life. Explicit and
1694 elaborate revocation mechanisms may be required for “public credentials” since these

1695 credentials are disseminated widely, possibly with a preset validity period. For example,
1696 public key certificates are revoked using Certificate Revocation Lists (CRLs) after the
1697 certificates are distributed.

1698 “Private credentials” are held closely by the CSP, and hence the revocation and destruction of
1699 these credentials is implemented easily through an update of the CSP’s local credential stores.
1700 Credentials that bind usernames/passwords are instantaneously revoked and destroyed if the CSP
1701 deletes its mapping between the username and the password. Certain types of tokens may need to
1702 be explicitly deleted or zeroized at the end of the credential life in order to permanently disable
1703 the token and prevent its unauthorized reuse. For example, a Multi-factor Hardware
1704 Cryptographic Token may need to be zeroized to ensure that all of the information pertaining to
1705 the Subscriber is deleted from the token.

1706 The CSP may be responsible for ensuring that hardware tokens are collected and cleared of any
1707 data when the Subscriber no longer has a need for its use. The CSP may establish policies for
1708 token collection to avoid the possibility of unauthorized use of the token after it is considered out
1709 of use. The CSP may destroy such collected tokens, or zeroize them to ensure that there are no
1710 remnants of information that can be used by an Attacker to derive the token value. For example, a
1711 Subscriber who is issued a hardware OTP token by a CSP may be required by policy to return the
1712 token to the CSP at the end of its life, or when the Subscriber’s association with that CSP
1713 terminates.

1714 e) *Records retention* – The CSP or its representative is responsible for maintaining a record of
1715 the registration, history, and status of each token and credential, including revocation. CSPs
1716 operated by or on behalf of executive branch agencies shall also follow either the General
1717 Records Schedule established by the National Archives and Records Administration or an
1718 agency-specific schedule as applicable. All other entities shall comply with their respective
1719 records retention policies in accordance with whatever laws apply to those entities. A
1720 minimum record retention period is required at Level 2 and above.

1721 f) *Security controls* – The CSP is responsible for implementing and maintaining appropriate
1722 security controls contained in NIST SP 800-53. The security control baseline for CSPs is
1723 specified in terms of a FIPS 200 impact level for each assurance level. (See Section 7.3,
1724 below.)

1725

1726 **7.2. Token and Credential Management Threats**

1727 Tokens and credentials can only be as strong as the strength of the management mechanisms used to secure
1728 them. The CSP is responsible for mitigating threats to the management operations described in the last
1729 section. Token and credential management threats are described below; they are categorized in accordance
1730 with the management activity to which they apply.

1731 These threats represent the potential to breach the confidentiality, integrity and availability of tokens and
1732 credentials during the CSP activities, and are listed below.

1733

1734

1735

1736
 1737

Table 8 - Token and Credential Management Threats

Token and Credential Management Activity	Threat/Attack	Example
Credential storage	Disclosure	Username and passwords stored in a system file are revealed.
	Tampering	The file that maps usernames to passwords within the CSP is hacked so that the mappings are modified, and existing passwords are replaced by passwords known to the Attacker.
Token and credential verification services	Disclosure	An Attacker is able to view requests and responses between the CSP and the Verifier.
	Tampering	An Attacker is able to masquerade as the CSP and provide bogus responses to the Verifier's password verification requests.
	Unavailability	The password file or the CSP is unavailable to provide password and username mappings.
		Public key certificates for Claimants are unavailable to the Verifier because the directory systems are down (for example for maintenance or as a result of a denial of service attack).
Token and credential issuance/renewal/re-issuance	Disclosure	Password renewed by the CSP for a Subscriber is copied by an Attacker as it is transported from the CSP to the Subscriber.
	Tampering	New password created by the Subscriber is modified by an Attacker as it is being submitted to the CSP to replace an expired password.
	Unauthorized issuance	The CSP is compromised through unauthorized physical or logical access resulting in issuance of fraudulent credentials.
	Unauthorized renewal/re-issuance	Attacker fools the CSP into re-issuing the credential for a current Subscriber – the new credential binds the current Subscriber's identity with a token provided by the Attacker.

Token and Credential Management Activity	Threat/Attack	Example
		Attacker is able to take advantage of a weak credential renewal protocol to extend the credential validity period for a current Subscriber.
Token and credential revocation/destruction	Delayed revocation/destruction of credentials	Stale CRLs allow accounts (that should have been locked as a result of credential revocation) to be used by an Attacker. User accounts are not deleted when employees leave a company leading to a possible use of the old accounts by unauthorized persons.
	Token use after decommissioning	A hardware token is used after the corresponding credential was revoked or expired.

1738

1739 **7.2.1. Threat Mitigation Strategies**

1740 Token and credential management related mechanisms that assist in mitigating the threats identified above
 1741 are summarized in Table 9.

1742 **7.3. Token and Credential Management Assurance Levels**

1743 **7.3.1. Requirements per Assurance Level**

1744 The stipulations for management of tokens and credentials by the CSP and Verifier are described below for
 1745 each assurance level. The stipulations described at each level in this section are incremental in nature;
 1746 requirements stipulated at lower levels are implicitly included at higher levels.

1747

1748
 1749

Table 9 - Token and Credential Threat Mitigation Strategies

Token and Credential Management Activity	Threat/Attack	Mitigation Strategy
Credential storage	Disclosure	Use access control mechanisms that protect against unauthorized disclosure of credentials held in storage.
	Tampering	Use access control mechanisms that protect against unauthorized tampering of credentials and tokens.
Token and credential verification services	Disclosure	Use a communication protocol that offers confidentiality protection.
	Tampering	Ensure that Verifiers authenticate the CSP prior to accepting a verification response from that CSP.
		Use a communication protocol that offers integrity protection.
	Unavailability	Ensure that the CSP has a well developed and tested Contingency Plan.
Token and credential issuance/renewal/re-issuance	Disclosure	Use a communication protocol that provides confidentiality protection of session data.
	Tampering	Use a communication protocol that allows the Subscriber to authenticate the CSP prior to engaging in token re-issuance activities and protects the integrity of the data passed.
	Unauthorized issuance	Implement physical and logical access controls to prevent compromise of the CSP. See [FISMA] for details on security controls.
	Unauthorized renewal/re-issuance	Establish policy that Subscriber shall prove possession of the old token to successfully negotiate the re-issuance process. Any attempt to negotiate the re-issuance process using an expired or revoked token should fail.
Credential revocation/destruction	Delayed revocation/destruction of credentials	Revoke/Destroy credentials as soon as notification that the credentials should be revoked or destroyed.
	Token use after decommissioning	Destroy tokens after their corresponding credentials have been revoked.

1750
 1751
 1752
 1753
 1754
 1755

7.3.1.1. Level 1

At Level 1, the following shall be required:

- a) *Credential storage* –
 - i) Files of shared secrets used by Verifiers at Level 1 authentication shall be protected by access controls that limit access to administrators and only to those applications that

- 1756 require access.
1757 [KI-IAF: AL1_CO_SCO#020 a)]
- 1758 ii) Such shared secret files shall not contain the plaintext passwords; typically they contain a
1759 one-way hash or “inversion” of the password.
1760 [KI-IAF: AL1_CO_SCO#020 b)]
- 1761 iii) In addition, any method allowed for the protection of long-term shared secrets at Level 2
1762 or above may be used at Level 1.
1763 [KI-IAF: Implicit]
- 1764 b) *Token and credential verification services* – Long term token secrets should not be shared
1765 with other parties unless absolutely necessary.
1766 [KI-IAF: The requirement is conditional in two terms, leading to subjectivity which, at AL1, does not justify a
1767 specific criterion]
- 1768 c) *Token and credential renewal / re-issuance* – No stipulation
- 1769 d) *Token and credential revocation and destruction* – No stipulation
- 1770 e) *Records retention* – No stipulation
- 1771 f) *Security controls* – No stipulation

1772

1773 7.3.1.2. Level 2

1774 At Level 2, the following shall be required:

- 1775 a) *Credential storage* –
- 1776 i) Files of shared secrets used by CSPs at Level 2 shall be protected by access controls that
1777 limit access to administrators and only to those applications that require access.
1778 [KI-IAF: AL2_CO_SCO#020 a)]
- 1779 ii) Such shared secret files shall not contain the plaintext passwords or secrets; two
1780 alternative methods may be used to protect the shared secret:
1781 [KI-IAF: AL2_CO_SCO#020 b) +NIST SP 800-63-2 Profiling]
- 1782 1) Passwords may be concatenated to a variable salt (variable across a group of
1783 passwords that are stored together) and then hashed with an Approved algorithm so
1784 that the computations used to conduct a dictionary or exhaustion attack on a stolen
1785 password file are not useful to attack other similar password files. The hashed
1786 passwords are then stored in the password file. The variable salt may be composed
1787 using a global salt (common to a group of passwords) and the username (unique per
1788 password) or some other technique to ensure uniqueness of the salt within the group of
1789 passwords.
- 1790 2) Shared secrets may be encrypted and stored using Approved encryption algorithms and
1791 modes, and the needed secret decrypted only when immediately required for
1792 authentication. In addition, any method allowed to protect shared secrets at Level 3 or
1793 4 may be used at Level 2.
- 1794 b) *Token and credential verification services* –
- 1795 i) Long term shared authentication secrets, if used:

- 1796 1) shall never be revealed to any other party except Verifiers operated by the CSP;
1797 however,
1798 [KI-IAF: AL2_CO_SCO#020 c)]
- 1799 2) session (temporary) shared secrets may be provided by the CSP to independent
1800 Verifiers.
1801 [KI-IAF: AL2_CO_SCO#020 c) – this would be the case if the Verifier was a separate Kantara-
1802 Approved CSP]
- 1803 ii) Cryptographic protections are required for all messages between the CSP and Verifier
1804 which contain private credentials or assert the validity of weakly bound or potentially
1805 revoked credentials.
1806 [KI-IAF: AL2_CO_SCO#010]
- 1807 iii) Private credentials shall only be sent through a protected session to an authenticated
1808 party to ensure confidentiality and tamper protection.
1809 [KI-IAF: AL2_CO_SCO#010]
- 1810 iv) The CSP may send the Verifier a message that either asserts that a weakly bound
1811 credential is valid, or that a strongly bound credential has not been subsequently
1812 revoked. In this case, the message shall be logically bound to the credential, and the
1813 message, the logical binding, and the credential shall all be transmitted within a single
1814 integrity-protected session between the Verifier and the authenticated CSP.
1815 [KI-IAF: AL2_CO_SCO#015]
- 1816 v) If revocation is required, the integrity-protected messages shall either be time stamped,
1817 or the session keys shall expire with an expiration time no longer than that of the
1818 revocation list. Alternatively, the time-stamped message, binding, and credential may all
1819 be signed by the CSP, although, in this case, the three in combination would comprise a
1820 strongly bound credential with no need for revocation.
1821 [KI-IAF: AL2_CM_RVP#045]
- 1822 c) *Token and credential renewal/re-issuance –*
- 1823 i) The CSP shall establish suitable policies for renewal and re-issuance of tokens and
1824 credentials.
1825 [KI-IAF: AL2_CO_NUI#020 a)]
- 1826 ii) Proof-of-possession of the unexpired current token shall be demonstrated by the
1827 Claimant prior to the CSP allowing renewal and re-issuance.
1828 [KI-IAF: AL2_CM_RNR#020]
- 1829 iii) Passwords shall not be renewed; they shall be re-issued. After expiry of current token
1830 and any grace period, renewal and re-issuance shall not be allowed. Upon re-issuance,
1831 token secrets shall not be set to a default or reused in any manner.
1832 [KI-IAF: AL2_CM_RNR#030 a), b), c)]
- 1833 iv) All interactions shall occur over a protected session such as SSL/TLS.
1834 [KI-IAF: AL2_CM_RNR#030 d)]
- 1835 d) *Token and credential revocation and destruction –*
- 1836 i) CSPs shall revoke or destroy credentials and tokens within 72 hours after being notified
1837 that a credential is no longer valid or a token is compromised to ensure that a Claimant
1838 using the token cannot successfully be authenticated.
1839 [KI-IAF: AL2_CM_RVP#030]

- 1840 ii) If the CSP issues credentials that expire automatically within 72 hours (e.g., issues fresh
1841 certificates with a 24 hour validity period each day) then the CSP is not required to
1842 provide an explicit mechanism to revoke the credentials.
1843 [KI-IAF: AL2_CM_RVP#030]
- 1844 iii) CSPs that register passwords shall ensure that the revocation or de-registration of the
1845 password can be accomplished in no more than 72 hours.
1846 [KI-IAF: AL2_CM_RVP#030]
- 1847 iv) CAs cross-certified with the Federal Bridge CA at the Citizen and Commerce Class
1848 Basic, Medium and High or Common Certificate Policy levels are considered to meet
1849 credential status and revocation provisions of this level.
1850 [KI-IAF: Therefore the above mappings apply.]
- 1851 e) *Records retention* –
- 1852 i) A record of the registration, history, and status of each token and credential (including
1853 revocation) shall be maintained by the CSP or its representative.
1854 [KI-IAF: AL2_CM_CSM#010, AL2_CM_RVP#050]
- 1855 ii) The record retention period of data for Level 2 credentials is seven years and six months
1856 beyond the expiration or revocation (whichever is later) of the credential.
1857 [KI-IAF: AL2_ID_VRC#030, AL2_CM_RNR#050, AL2_CM_RVP#060]
- 1858 iii) CSPs operated by or on behalf of executive branch agencies shall also follow either the
1859 General Records Schedule established by the National Archives and Records
1860 Administration or an agency-specific schedule as applicable. All other entities shall
1861 comply with their respective records retention policies in accordance with whatever laws
1862 apply to those entities.
1863 [KI-IAF: AL2_CO_ESM#030, 'ESM#050+NIST SP 800-63-2 Profiling (in each case)]
- 1864 f) *Security controls* – The CSP must employ appropriately-tailored security controls from the
1865 low baseline of security controls defined in [SP 800-53] and must ensure that the minimum
1866 assurance requirements associated with the low baseline are satisfied.
1867 [KI-IAF: AL2_CO_ISM#030, AL2_CO_ISM#070, AL2_CO_ISM#080, AL2_CO_SER#010, AL2_CO_OPN#010,
1868 AL2_CO_SCO#020 +NIST SP 800-63-2 Profiling (in each case)]

1869 7.3.1.3. Level 3

1870 At Level 3, the following ~~is~~ shall be required:

- 1871 a) *Credential storage*²⁷ –
- 1872 i) Files of long-term shared secrets used by CSPs or Verifiers at Level 3 shall be protected
1873 by access controls that limit access to administrators and only to those applications that
1874 require access.
1875 [KI-IAF: AL3_CO_SCO#020 a), c)]
- 1876 ii) Such shared secret files shall be encrypted so that:
1877 [KI-IAF: AL3_CO_SCO#020 b i) & ii)]
- 1878 1) The encryption key for the shared secret file is encrypted under a key held in a FIPS
1879 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-
1880 2 Level 3 or 4 cryptographic module and decrypted only as immediately required
1881 for an authentication operation;

²⁷ With regard to references to FIPS 140-2, products validated under subsequent versions of FIPS 140-2 are also acceptable.

- 1882 2) Shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2
1883 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4
1884 cryptographic module and is not exported in plaintext from the module.
- 1885 ii) Strongly bound credentials support tamper detection mechanisms such as digital
1886 signatures, but weakly bound credentials can be protected against tampering using
1887 access control mechanisms as described above.
1888 *[KI-IAF: given the absence of any imperative requirement, this is considered tutorial.]*
1889
- 1890 b) *Token and credential verification services –*
- 1891 i) CSPs shall provide a secure mechanism to allow Verifiers or RPs to ensure that the
1892 credentials are valid.
1893 *[KI-IAF: AL3_CM_ASS#010, AL3_CM_ASS #015*
- 1894 ii) Such mechanisms may include on-line validation servers or the involvement of CSP
1895 servers that have access to status records in authentication transactions.
1896 *[KI-IAF: Implicit, in that Kantara recognizes CSPs which may not be fulfilling all 100% of SAC at any*
1897 *given AL(s)]*
- 1898 iii) Temporary session authentication keys may be generated from long-term shared secret
1899 keys by CSPs and distributed to third party Verifiers, as a part of the verification
1900 services offered by the CSP, but long-term shared secrets shall not be shared with any
1901 third parties, including third party Verifiers.
1902 *[KI-IAF: AL3_CO_SCO#020 a). Kantara does not fully enforce the above clause – see*
1903 *AL3_CO_SCO#020 c). NIST SP 800-63-2 Profiling would be required to ensure compliance (application*
1904 *of this limitation would not conflict with AL3_CO_SCO#020 and c)).]*
1905
1906 *[KI-IAF: the following paragraph is considered tutorial.]*
1907 This type of third-party (or delegated) verification is used in the realm of GSM (Global
1908 System for Mobile Communications) roaming; the locally available network
1909 authenticates the “roaming” Subscriber using a temporary session authentication key
1910 received from the Base Station. Such temporary session authentication keys are typically
1911 created by cryptographically combining the long term shared secret with a nonce
1912 challenge, to generate a session key. The challenge and session key are securely
1913 transmitted to the Verifier. The Verifier in turn sends only the challenge to the Claimant,
1914 and the Claimant applies the challenge to the long-term shared secret to generate the
1915 session key. Both Claimant and Verifier now share a session key, which can be used for
1916 authentication. Such verification schemes are permitted at this level provided that
1917 Approved cryptographic algorithms are used for all operations.
- 1918 iv) Token and credential verification services categorized as FIPS 199 “Moderate” or
1919 “High” for availability shall be protected in accordance with the Contingency Planning
1920 (CP) controls specified in NIST SP 800-53 to provide an adequate level of availability
1921 needed for the service.
1922 *[KI-IAF: AL3_CO_ISM#030, AL3_CO_ISM#070, AL3_CO_ISM#080, AL3_CO_OPN#010 +NIST SP*
1923 *800-63-2 Profiling (in each case)]*
- 1924 c) *Token and credential renewal /re-issuance –*
- 1925 i) The CSP shall establish suitable policies for renewal and re-issuance of tokens and
1926 credentials.
1927 *[KI-IAF: AL3_CO_NUI#020 a) NOTE – SP 800-63-2 has no explicit requirement such as this at AL3,*
1928 *which seems an oversight.]*

- 1929 ii) Renewal and re-issuance shall only occur prior to expiration of the current credential.
1930 Claimants shall be authenticated by the CSP using the existing token and credential in
1931 order to renew or re-issue the credential.
1932 [KI-IAF: AL3_CM_RNR#020]
- 1933 iii) All interactions shall occur over a protected session such as SSL/TLS.
1934 [KI-IAF: AL3_CM_RNR#030 d)]
- 1935 d) *Credential revocation and destruction* –
- 1936 i) CSPs shall have a procedure to revoke credentials and tokens within 24 hours.
1937 [KI-IAF: AL3_CM_RVP#030]
- 1938 ii) The certificate status provisions of CAs cross-certified with the Federal Bridge CA at the
1939 Basic, Medium, High or Common Certificate Policy levels are considered to meet
1940 credential status and revocation provisions of this level.
1941 [KI-IAF: Therefore the above mappings apply.]
- 1942 iii) Verifiers shall ensure that the tokens they rely upon are either freshly issued (within 24
1943 hours) or still valid.
1944 [KI-IAF: AL3_CM_ASS#018]
- 1945 iv) Shared secret-based authentication systems may simply remove revoked Subscribers
1946 from the verification database.
1947 [KI-IAF: This is effectively an option, hence no criterion applies.]
- 1948 e) *Records retention* –
- 1949 i) A record of the registration, history, and status of each token and credential (including
1950 revocation) shall be maintained by the CSP or its representative.
1951 [KI-IAF: AL3_CM_CSM#010, AL3_CM_RVP#050]
- 1952 ii) The record retention period of data for Level 3 credentials is seven years and six months
1953 beyond the expiration or revocation (whichever is later) of the credential.
1954 [KI-IAF: AL3_ID_VRC#030, AL3_CM_RNR#050, AL3_CM_RVP#060]
- 1955 iii) CSPs operated by or on behalf of executive branch agencies shall also follow either the
1956 General Records Schedule established by the National Archives and Records
1957 Administration or an agency-specific schedule as applicable. All other entities shall
1958 comply with their respective records retention policies in accordance with whatever laws
1959 apply to those entities.
1960 [KI-IAF: AL3_CO_ESM#030, AL3_CO_ESM#050, AL3_CM_RVP#060+NIST SP 800-63-2 Profiling (in
1961 each case)]
- 1962 f) *Security controls* – The CSP must employ appropriately-tailored security controls from the
1963 moderate baseline of security controls defined in [SP 800-53] and must ensure that the
1964 minimum assurance requirements associated with the moderate baseline are satisfied.
1965 [KI-IAF: AL3_CO_ISM#030, AL3_CO_ISM#070, AL3_CO_ISM#080, AL3_CO_SER#010, AL3_CO_OPN#010,
1966 AL3_CO_SCO#020+NIST SP 800-63-2 Profiling (in each case)]

1967 7.3.1.4. Level 4

1968 At Level 4, the following is shall be required:

- 1969 a) *Credential storage* – All stipulations from Level 3 apply.
1970 [KI-IAF: All mappings at AL3 apply, save amendment to refer to AL4... criteria]
- 1971 b) *Token and credential verification services* – All stipulations from Level 3 apply.
1972 [KI-IAF: All mappings at AL3 apply, save amendment to refer to AL4... criteria]

- 1973
- 1974
- 1975
- 1976
- 1977
- 1978
- 1979
- 1980
- 1981
- 1982
- 1983
- 1984
- 1985
- 1986
- 1987
- 1988
- 1989
- 1990
- 1991
- 1992
- 1993
- 1994
- 1995
- 1996
- 1997
- 1998
- 1999
- 2000
- 2001
- 2002
- 2003
- 2004
- 2005
- 2006
- 2007
- 2008
- 2009
- 2010
- 2011
- 2012
- 2013
- 2014
- 2015
- 2016
- 2017
- 2018
- c) *Token and credential renewal/re-issuance* –
- i) The CSP shall establish suitable policies for renewal and re-issuance of tokens and credentials.
[KI-IAF: AL4_CO_NUI#020 a) NOTE – SP 800-63-2 has no explicit requirement such as this at AL3, which seems an oversight.]
- ii) Sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process.
[KI-IAF: AL4_CM_CTR#030 d)]
- iii) All temporary or short-term keys derived during the ~~initial~~ ~~original~~ authentication operation shall expire and re-authentication shall be required after not more than 24 hours from the initial authentication.
[KI-IAF: AL4_CM_RNR#040]
- d) *Token and credential revocation and destruction* –
- i) CSPs shall ~~have a procedure to~~ revoke credentials within 24 hours.
[KI-IAF: AL4_CM_RVP#030]
- ii) The certificate status provisions of CAs cross-certified with the Federal Bridge CA at the High and Common Certificate Policies shall be considered to meet credential status provisions of Level 4. [FBCA1]
[KI-IAF: Therefore the above mappings apply.]
- iii) Verifiers or RPs shall ensure that the credentials they rely upon are either freshly issued (within 24 hours) or still valid.
[KI-IAF: AL4_CM_ASS#018]
- iv) It is generally good practice to destroy a token within 48 hours of the end of its life or the end of the Subscriber’s association with the CSP. Destroying includes either the physical destruction of the token or cleansing it of all information related to the Subscriber.
[KI-IAF: This is effectively an option/tutorial, hence no criterion applies.]
- e) *Records retention* –
- i) A record of the registration, history, and status of each token and credential (including revocation) shall be maintained by the CSP or its representative.
[KI-IAF: AL4_CM_CSM#010, AL4_CM_RVP#050]
- ii) The record retention period of data for Level ~~2-4~~ credentials is ten years and six months beyond the expiration or revocation (whichever is later) of the credential.
[KI-IAF: AL4_ID_VRC#030, AL4_CM_RNR#050, AL4_CM_RVP#060]
- iii) CSPs operated by or on behalf of executive branch agencies shall also follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.
[KI-IAF: AL4_CO_ESM#030, AL4_CO_ESM#050, AL4_CM_RVP#060+NIST SP 800-63-2 Profiling (in each case)]
- f) *Security controls* – The CSP must employ appropriately-tailored security controls from the moderate baseline of security controls defined in [SP 800-53] and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.
[KI-IAF: AL4_CO_ISM#030, AL4_CO_ISM#070, AL4_CO_ISM#080, AL4_CO_SER#010, AL4_CO_OPN#010, AL4_CO_SCO#020 +NIST SP 800-63-2 Profiling (in each case)]

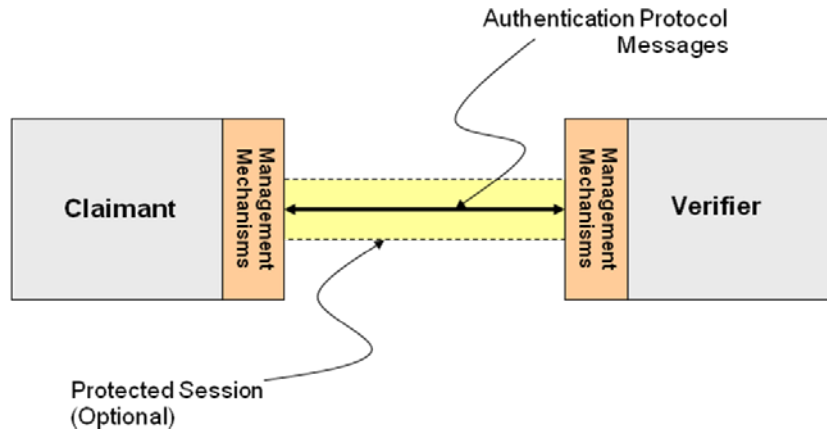
- 2019 **7.3.2. Relationship of PKI Policies to E-Authentication Assurance Levels**
- 2020 Appendix B specifies the mapping between the Federal PKI Certificate Policies and the requirements in
- 2021 Section 7.
- 2022 [*KI-IAF: +NIST SP 800-63-2 Profiling*]

2023

2024 8. Authentication Process

2025 8.1. Overview

2026 The authentication process establishes the identity of the Claimant to the Verifier with a certain degree of
2027 assurance. It is implemented through an authentication protocol message exchange, as well as management
2028 mechanisms at each end that further constrain or secure the authentication activity. One or more of the
2029 messages of the authentication protocol may need to be carried on a protected session. This is illustrated in
2030 Figure 3.
2031



2032
2033
2034
2035

Figure 3 - *Authentication Process Model*

2036 *An authentication protocol is a defined sequence of messages between a Claimant and a Verifier that*
2037 *demonstrates that the Claimant has control of a valid token to establish his or her identity, and optionally,*
2038 *demonstrates to the Claimant that he or she is communicating with the intended Verifier. An exchange of*
2039 *messages between a Claimant and a Verifier that results in authentication (or authentication failure) between*
2040 *the two parties is an authentication protocol run. During or after a successful authentication protocol run, a*
2041 *protected communication session may be created between the two parties; this protected session may be used*
2042 *to exchange the remaining messages of the authentication protocol run, or to exchange session data between*
2043 *the two parties.*

2044 Management mechanisms may be implemented on the Claimant and the Verifier to further enhance the
2045 authentication process. For example, trust anchors may be established at the Claimant to enable the
2046 authentication of the Verifier using public key mechanisms such as TLS. Similarly, mechanisms may be
2047 implemented on the Verifier to limit the rate of online guessing of passwords by an Attacker who is trying to
2048 authenticate as a legitimate Claimant. Further, detection of authentication transactions originating from an
2049 unexpected location or channel for a Claimant, or indicating use of an unexpected hardware or software
2050 configuration, may indicate increased risk levels and motivate additional confirmation of the Claimant's
2051 identity.

2052 At the conclusion of the authentication protocol run, the verifier might issue a secondary authentication
2053 credential, such as a cookie, to the Claimant and rely upon it to authenticate the claimant in the near future.
2054 Requirements for doing this securely are in Section 9.

2055 **8.2. Authentication Process Threats**

2056 In general, attacks that reveal long-term token secrets are worse than attacks that reveal short-term
 2057 authentication secrets or session data, because in the former, the Attacker can then use the token secret to
 2058 assume a Subscriber’s identity and do greater harm.

2059 RAs, CSPs, and Verifiers are ordinarily trustworthy (in the sense of being correctly implemented and not
 2060 deliberately malicious). However, Claimants or their systems may not be trustworthy (or else their identity
 2061 claims could simply be trusted). Moreover, while RAs, CSPs, and Verifiers are normally trustworthy, they
 2062 are not invulnerable, and could become corrupted. Therefore, authentication protocols that expose long-term
 2063 authentication secrets more than is absolutely required, even to trusted entities, should be avoided. Table 10
 2064 lists the types of threats posed to the authentication process.

2065 Table 10 - Authentication Process Threats

Type of Attack	Description	Example
Online guessing	An Attacker performs repeated logon trials by guessing possible values of the token authenticator.	An Attacker navigates to a web page and attempts to log in using a Subscriber's username and commonly used passwords, such as "password" and "secret".
Phishing	A Subscriber is lured to interact with a counterfeit Verifier, and tricked into revealing his or her token secret, sensitive personal data or authenticator values that can be used to masquerade as the Subscriber to the Verifier.	A Subscriber is sent an email that redirects him or her to a fraudulent website and is asked to log in using his or her username and password.
Pharming	A Subscriber who is attempting to connect to a legitimate Verifier, is routed to an Attacker’s website through manipulation of the domain name service or routing tables.	A Subscriber is directed to a counterfeit website through DNS poisoning, and reveals or uses his or her token believing he or she is interacting with the legitimate Verifier.
Eavesdropping	An Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant.	An Attacker captures the transmission of a password or password hash from a Claimant to a Verifier.
Replay	An Attacker is able to replay previously captured messages (between a legitimate Claimant and a Verifier) to authenticate as that Claimant to the Verifier.	An Attacker captures a Claimant’s password or password hash from an actual authentication session, and replays it to the Verifier to gain access at a later time.
Session hijack	An Attacker is able to insert himself or herself between a Subscriber and a Verifier subsequent to a successful authentication exchange between the latter two parties. The Attacker is able to pose as a Subscriber to the Verifier/RP or vice versa to control session data exchange.	An Attacker is able to take over an already authenticated session by eavesdropping on or predicting the value of authentication cookies used to mark HTTP requests sent by the Subscriber.

Type of Attack	Description	Example
Man-in-the-middle	The Attacker positions himself or herself in between the Claimant and Verifier so that he or she can intercept and alter the content of the authentication protocol messages. The Attacker typically impersonates the Verifier to the Claimant and simultaneously impersonates the Claimant to the Verifier. Conducting an active exchange with both parties simultaneously may allow the Attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other.	An Attacker breaks into a router that forwards messages between the Verifier and a Claimant. When forwarding messages, the Attacker substitutes his or her own public key for that of the Verifier. The Claimant is tricked into encrypting his or her password so that the Attacker can decrypt it. An Attacker sets up a fraudulent website impersonating the Verifier. When an unwary Claimant tries to log in using his or her one-time password device, the Attacker's website simultaneously uses the Claimant's one-time password to log in to the real Verifier.

2066

2067 **8.2.1. Other Threats**

2068 Attacks are not limited to the authentication protocol itself. Other attacks include:

- 2069 a) Denial of Service attacks in which the Attacker overwhelms the Verifier by flooding it with a
- 2070 large amount of traffic over the authentication protocol;
- 2071 b) Malicious code attacks that may compromise or otherwise exploit authentication tokens;
- 2072 c) Attacks that fool Claimants into using an insecure protocol, when the Claimant thinks that he
- 2073 or she is using a secure protocol, or trick the Claimant into overriding security controls (for
- 2074 example, by accepting server certificates that cannot be validated).

2075 The purpose of flooding attacks is to overwhelm the resources used to support an authentication protocol to

2076 the point where legitimate Claimants cannot reach the Verifier or to slow down the process to make it more

2077 difficult for the Claimant to reach the Verifier. For example, a Verifier that implements an authentication

2078 protocol that uses encryption/decryption is sent a large number of protocol messages causing the Verifier to

2079 be crippled due to the use of excessive system resources to encrypt/decrypt. Nearly all authentication

2080 protocols are susceptible to flooding attacks; possible ways to resist such attacks is through the use of

2081 distributed Verifier architectures, use of load balancing techniques to distribute protocol requests to multiple

2082 mirrored Verifier systems, or other similar techniques.

2083 Malicious code could be introduced into the Claimant's computer system for the purpose of compromising or

2084 otherwise exploiting the Claimant's token. The malicious code may be introduced by many means, including

2085 the threats detailed below. There are many countermeasures (e.g., virus checkers and firewalls) that can

2086 mitigate the risk of malicious code on Claimant systems. General good practice to mitigate malicious code

2087 threats is outside the scope of this document²⁸. Hardware tokens prevent malicious software from extracting

2088 and copying the token secret. However, malicious code may still misuse the token, particularly if activation

2089 data is presented to the token via the computer.

²⁸ See SP 800-53, *Recommended Security Controls For Federal Information Systems*

2090 **8.2.2. Threat Mitigation Strategies**

2091 The following are strategies that can be incorporated in authentication processes to mitigate the attacks listed
2092 in the previous section:

- 2093 a) *Online guessing resistance* – An authentication process is resistant to online guessing attacks
2094 if it is impractical for the Attacker, with no a priori knowledge of the token authenticator, to
2095 authenticate successfully by repeated authentication attempts with guessed authenticators. The
2096 entropy of the authenticator, the nature of the authentication protocol messages, and other
2097 management mechanisms at the Verifier contribute to this property. For example, password
2098 authentication systems can make targeted password guessing impractical by requiring use of
2099 high-entropy passwords and limiting the number of unsuccessful authentication attempts, or
2100 by controlling the rate at which attempts can be carried out. (See Appendix A and Tables 6-1
2101 to 6-4 in Section 6.3.1.). Similarly, to resist untargeted password attacks, a Verifier may
2102 supplement these controls with network security controls.
- 2103 b) *Phishing and pharming resistance (verifier impersonation)* – An authentication process is
2104 resistant to phishing and pharming (also known as Verifier impersonation,) if the impersonator
2105 does not learn the value of a token secret or a token authenticator that can be used to act as a
2106 Subscriber to the genuine Verifier. In the most general sense, this assurance can be provided
2107 by the same mechanisms that provide the strong man-in-the-middle resistance described later
2108 in this section; however, long term secrets can be protected against phishing and pharming
2109 simply by the use of a tamper resistant token, provided that the long term secret cannot be
2110 reconstructed from a Token Authenticator. To decrease the likelihood of phishing and
2111 pharming attacks, it is recommended that the Claimant authenticate the Verifier using
2112 cryptographic mechanisms prior to submitting the token authenticator to the supposed
2113 Verifier. Additionally, management mechanisms can be implemented at the Verifier to send a
2114 Claimant personalized content after successful authentication of the Claimant or the
2115 Claimant’s device. (Refer to Section 8.2.4 for further details on personalization.) This allows
2116 the Claimant to achieve a higher degree of assurance of the authenticity of the Verifier before
2117 proceeding with the remainder of the session with the Verifier or RP. It should be mentioned,
2118 however, that there is no foolproof way to prevent the Claimant from revealing any sensitive
2119 information to which he or she has access.
- 2120 c) *Eavesdropping resistance* – An authentication process is resistant to eavesdropping attacks if
2121 an eavesdropper who records all the messages passing between a Claimant and a Verifier
2122 finds it impractical to learn the Claimant’s token secret or to otherwise obtain information that
2123 would allow the eavesdropper to impersonate the Subscriber in a future authentication session.
2124 Eavesdropping-resistant protocols make it impractical²⁹ for an Attacker to carry out an off-line
2125 attack where he or she records an authentication protocol run and then analyzes it on his or her
2126 own system for an extended period to determine the token secret or possible token
2127 authenticators. For example, an Attacker who captures the messages of a password-based
2128 authentication protocol run may try to crack the password by systematically trying every
2129 password in a large dictionary, and comparing it with the protocol run data. Protected session
2130 protocols, such as TLS, provide eavesdropping resistance.

²⁹ “Impractical” is used here in the cryptographic sense of nearly impossible, that is there is always a small chance of success, but even the Attacker with vast resources will nearly always fail. For off-line attacks, impractical means that the amount of work required to “break” the protocol is at least on the order of 2^{80} cryptographic operations. For on-line attacks impractical means that the number of possible on-line trials is very small compared to the number of possible key or password values.

- 2131 d) *Replay resistance* – An authentication process resists replay attacks if it is impractical to
2132 achieve a successful authentication by recording and replaying a previous authentication
2133 message. Protocols that use nonces or challenges to prove the “freshness” of the transaction
2134 are resistant to replay attacks since the Verifier will easily detect that the old protocol
2135 messages replayed do not contain the appropriate nonces or timeliness data related to the
2136 current authentication session.
- 2137 e) *Hijacking resistance* – An authentication process and data transfer protocol combination are
2138 resistant to hijacking if the authentication is bound to the data transfer in a manner that
2139 prevents an adversary from participating actively in the data transfer session between the
2140 Subscriber and the Verifier or RP without being detected. This is a property of the relationship
2141 of the authentication protocol and the subsequent session protocol used to transfer data. This
2142 binding is usually accomplished by generating a per-session shared secret during the
2143 authentication process that is subsequently used by the Subscriber and the Verifier or RP to
2144 authenticate the transfer of all session data.

2145
2146 It is important to note that web applications, even those protected by SSL/TLS, can still be
2147 vulnerable to a type of session hijacking attack called Cross Site Request Forgery (CSRF). In this
2148 type of attack, a malicious website contains a link to the URL of the legitimate RP. The malicious
2149 website is generally constructed so that a web browser will automatically send an HTTP request
2150 to the RP whenever the browser visits the malicious website. If the Subscriber visits the malicious
2151 website while he or she has an open SSL/TLS session with the RP, the request will generally be
2152 sent in the same session and with any authentication cookies intact. While the Attacker never
2153 gains access to the session secret, the request may be constructed to have side effects, such as
2154 sending an email message or authorizing a large transfer of money.

2155
2156 CSRF attacks may be prevented by making sure that neither an Attacker nor a script running on
2157 the Attacker’s website has sufficient information to construct a valid request authorizing an action
2158 (with significant consequences) by the RP. This can be done by inserting random data, supplied
2159 by the RP, into any linked URL with side effects and into a hidden field within any form on the
2160 RP’s website. This mechanism, however, is not effective if the Attacker can run scripts on the
2161 RP’s website (Cross Site Scripting or XSS). To prevent XSS vulnerabilities, the RP should
2162 sanitize inputs from Claimants or Subscribers to make sure they are not executable, or at the very
least not malicious, before displaying them as content to the Subscriber’s browser.

- 2163 f) *Man-in-the-middle resistance* – Authentication protocols are resistant to a man-in-the-middle
2164 attack when both parties (i.e., Claimant and Verifier) are authenticated to the other in a
2165 manner that prevents the undetected participation of a third party. There are two levels of
2166 resistance:
- 2167 i) *Weak man-in-the-middle resistance* – A protocol is said to be weakly resistant to man-
2168 in-the-middle attacks if it provides a mechanism for the Claimant to determine whether
2169 he or she is interacting with the real Verifier, but still leaves the opportunity for the non-
2170 vigilant Claimant to reveal a token authenticator (to an unauthorized party) that can be
2171 used to masquerade as the Claimant to the real Verifier. For example, sending a
2172 password over server authenticated TLS is weakly resistant to man-in the middle attacks.
2173 The browser allows the Claimant to verify the identity of the Verifier; however, if the
2174 Claimant is not sufficiently vigilant, the password will be revealed to an unauthorized
2175 party who can abuse the information. Weak man-in-the-middle resistance can also be
2176 provided by a zero-knowledge password protocol, such as Encrypted Key Exchange

2177 (EKE), Simple Password Exponential Key Exchange (SPEKE), or Secure Remote
2178 Password Protocol (SRP), which enables the Claimant to authenticate to a Verifier
2179 without disclosing the token secret. However, it is possible for the Attacker to trick the
2180 Claimant into passing his or her password into a less secure protocol, thereby revealing
2181 the password to the Attacker. Furthermore, if it is unreasonably difficult for the Claimant
2182 to verify that the proper protocol is being used, then the overall authentication process
2183 does not even provide weak man-in-the-middle resistance (for example, if a zero-
2184 knowledge password protocol is implemented by an unsigned java applet displayed on a
2185 plaintext HTTP page).

2186 ii) *Strong man-in-the-middle resistance*: A protocol is said to be strongly resistant to man-
2187 in-the-middle attack if it does not allow the Claimant to reveal, to an Attacker
2188 masquerading as the Verifier, information (token secrets, authenticators) that can be
2189 used by the latter to masquerade as the true Claimant to the real Verifier. An example of
2190 such a protocol is client authenticated TLS, where the browser and the web server
2191 authenticate one another using PKI. Even an unwary Claimant cannot easily reveal to an
2192 Attacker masquerading as the Verifier any information that can be used by the Attacker
2193 to authenticate to the real Verifier. Specialized protocols where the Claimant's token
2194 device will only release an authenticator to a preset list of valid Verifiers may also be
2195 strongly resistant to man-in-the-middle attacks.

2196 Note that systems can supplement the mitigation strategies listed above by enforcing appropriate security
2197 policies. For example, device identity, system health checks, and configuration management can be used to
2198 mitigate the risk that the Claimant's system has been compromised.
2199

2200 **8.2.3. Throttling Mechanisms**

2201 When using a token that produces low entropy token Authenticators, it is necessary to implement controls at
2202 the Verifier to protect against online guessing attacks. An explicit requirement for such tokens is given in
2203 Tables 6-1 to 6-4: the Verifier shall effectively limit online Attackers to 100 failed attempts on a single
2204 account in any 30 day period.

2205 The simplest way of implementing a throttling mechanism (which is not the recommended approach) would
2206 be to keep a counter of failed attempts that is reset at the beginning of each calendar month, and to lock the
2207 account for the rest of the month, when the counter exceeds 50. Aside from the fact that this system would
2208 not technically meet the requirement on the first of March in non-leap years, this throttling mechanism has a
2209 number of more severe problems. Most notably, it leaves the Verifier open to a very easy denial of service
2210 attack (on the first day of the month, an Attacker simply makes 50 failed attempts on each Subscriber account
2211 he or she knows about, and the system is unusable for the next 29 days.)

2212 The above simple implementation is also sufficiently limiting that it may suffer from usability problems,
2213 where the legitimate Subscriber is penalized for behavior that could reasonably be identified as benign and
2214 should not be counted as failed attempts by an Attacker. For example, if the Verifier records a dozen failed
2215 authentication attempts followed by a successful attempt from the same IP address over a few minutes to a
2216 few hours, it would be reasonable to assume that those attempts did not come from an Attacker.

2217 Additional techniques can be used to prioritize authentication attempts that are likely to come from the
2218 Subscriber over those that are more likely to come from an Attacker.

- 2219 a) Requiring the Claimant to complete a Completely Automated Public Turing test to tell
2220 Computers and Humans Apart (CAPTCHA) before attempting authentication.
- 2221 b) Requiring the Claimant to wait for a short period of time (anything from 30 seconds to an
2222 hour, depending on how close the system is to its maximum allowance for failed attempts)
2223 before attempting Authentication following a failed attempt.
- 2224 c) Only accepting authentication requests from a white list of IP addresses at which the
2225 Subscriber has been successfully authenticated before.

2226 Since these measures often create user inconvenience, it is best to allow a certain number of failed
2227 authentication attempts before employing the above techniques. For example, a system which enforces the
2228 30-day failed attempt limit, by dividing the calendar into 10-day sub-periods and only allowing 25 failed
2229 attempts in each sub-period, could allocate failed attempts as follows: in a given 10 day period, the Verifier
2230 could allow 2 failed attempts each day regardless of any other considerations, allow an additional 5 failed
2231 attempts over the whole period with no additional protections, require CAPTCHAs for the next 5 failed
2232 attempts (beyond the 2-per-day quota), and only allow the final 5 attempts to come from a white-listed IP
2233 address after the Claimant has completed a CAPTCHA.

2234 Finally, if the Verifier accepts authentication attempts for a large number of Subscribers, it is possible that an
2235 Attacker will attempt on online attack on all Subscriber accounts simultaneously, hoping to gain access to
2236 one of them, thus circumventing the throttling mechanisms employed on the individual accounts. No specific
2237 guideline is given for protecting against such attacks, but Verifiers with a large number of Subscribers should
2238 take measures to detect such attacks and either respond to them automatically or alert system administrators
2239 to the threat.

2240 **8.2.4. Phishing and Pharming (Verifier Impersonation): Supplementary** 2241 **Countermeasures**

2242 It is important to note that phishing and pharming are attacks that use different techniques to achieve the
2243 same goal. Effectively, the Claimant is tricked into believing that he or she is interacting with the Verifier
2244 when in actuality, the Verifier is being impersonated by an Attacker attempting to collect token information
2245 or other sensitive information.

2246 In a successful phishing attack, the Attacker sends an official looking email to a Subscriber claiming to be a
2247 Verifier. The email usually contains a link to a counterfeit Verifier and will ask the Subscriber to click on the
2248 link and authenticate to the Verifier³⁰. The Subscriber proceeds to authenticate to the counterfeit Verifier and
2249 the login information and token authenticator is captured. At this point, the Subscriber is unaware that he or
2250 she has been phished, and proceeds with the actions requested by the original email. Once the Subscriber logs
2251 off, he or she is unaware that his or her login information has been captured and that potentially sensitive
2252 data has been captured.

2253 In a successful pharming attack, the Attacker corrupts either the domain name service (using a technique
2254 called DNS poisoning) or the local routing tables (by modifying the host files on a Claimant's computer to
2255 point to a bogus DNS server). When the Subscriber attempts to connect to a legitimate Verifier on the
2256 Internet, the corrupted DNS tables or routing tables take the Subscriber to a counterfeit Verifier on the

³⁰ Some phishing attacks may request the Subscriber to provide personally sensitive information so that the Attacker may impersonate the Subscriber outside the scope of E-authentication.

2257 Internet. The Subscriber unknowingly reveals token authenticators and other sensitive information to the
2258 counterfeit Verifier.

2259 The strongest mechanism for preventing phishing and pharming of authentication secrets, such as token
2260 authenticators, is to make sure that some authentication secrets are not directly accessible to the Claimant (as
2261 described in Section 8.2.2). However, to help mitigate a wider variety of phishing and pharming attacks, the
2262 following techniques may be used:

- 2263 a) *Out of band confirmation of transaction details* – Details (e.g., account number, amount) of
2264 sensitive transactions authorized by the Subscriber may be sent by the RP to the Subscriber’s
2265 out of band token and displayed along with a confirmation code. The confirmation code may
2266 either be cryptographically derived from the Subscriber’s token secret and the transaction
2267 details, or it may be a random value that is sent to the Subscriber’s out of band token along
2268 with the transaction details. Alternatively, transaction details may be typed in by the
2269 Subscriber as manual inputs to a one-time password device. In order to complete the
2270 transaction, the Subscriber shall send the correct one-time password or confirmation code to
2271 the Verifier or RP.
- 2272 b) *Adding a “Last Login” feature by the Verifier to inform the Subscriber of his or her last login*
2273 – If the Subscriber logged in at 8:00am and then logs in at 4:00pm but the Last Login feature
2274 states that the last login was at 2:00pm, the Subscriber may suspect that he or she has been
2275 phished and take appropriate action.

2276

2277 Personalization is the process of customizing a webpage or email for a user to enhance the user experience.
2278 For the purpose of this document, personalization schemes can assist the user to determine if he or she is
2279 interacting with the correct entity. It is important to note that personalization is at best a low assurance
2280 mechanism for mitigating Phishing and Pharming threats, especially when delivered over a communication
2281 protocol that is not strongly resistant to man-in-the-middle attacks. However, personalization may provide
2282 additional assurance when combined with other techniques.

2283 There are three types of personalization in the context of this guideline:

- 2284 a) *Pre-authentication personalization* – The Verifier displays to the Claimant some
2285 personalized indicator (such as an image or user-chosen phrase picked at registration) prior
2286 to the latter submitting the token authenticator to the former. This indicator may be
2287 established by the Subscriber at the time of registration. When the Claimant views the
2288 personalized indicator, the Claimant has an increased sense of assurance that he or she is
2289 interacting with the correct Verifier. For example, a Verifier may require the Claimant to
2290 submit the username first; in response, the Verifier provides the personalized indicator for
2291 the claimed username. If the Claimant recognizes the personalized indicator as his or her
2292 own, the Claimant submits his or her token authenticator to the Verifier. Pre-authentication
2293 personalization does not eliminate Phishing attacks, but requires the Attacker to use a more
2294 complex technique to succeed in a Phishing attack.
- 2295 b) *Post-authentication personalization* – The Verifier displays a personalized indicator to the
2296 Subscriber after successful authentication of the latter. The personalized indicator provides
2297 assurance to the Subscriber that he or she has in fact logged in to the correct site. This
2298 indicator may be established by the Subscriber at the time of registration. For example, after
2299 a Subscriber authenticates to the Verifier, the Verifier provides a personalized indicator (such
2300 as a picture, a phrase, or a greeting) that the Subscriber can readily recognize as his or her

2301 own. If the personalized indicator is not shown, or is not recognized by the Subscriber, the
2302 Subscriber suspects that he or she has been phished and takes appropriate action. Post-
2303 authentication personalization does not protect any secrets used by the Subscriber in the
2304 initial authentication process. Nonetheless, if some or all of these secrets are protected by
2305 hardware or software that runs a protocol with strong man-in-the-middle resistance, then the
2306 personalization will assist the Subscriber in recognizing that he or she is interacting with a
2307 bogus site and refraining from revealing any further sensitive information. If personalization
2308 appears before the Subscriber is prompted for a password, but after the Verifier strongly
2309 authenticates the Subscriber's local system, then the Subscriber's password may also be
2310 protected from phishing.

- 2311 c) *Personalization of email sent to the Subscriber by a valid Verifier* – This type of
2312 personalization is employed to help the Subscriber differentiate between email from a valid
2313 Verifier, and email from a Phisher. For example, an email from a Verifier may contain a
2314 picture which the Subscriber selected in the registration process. This type of personalization
2315 forces the Phisher to use a fairly difficult attack and in effect forces the Phisher to either use
2316 a targeted attack against each Subscriber or hope that the Subscriber will not notice the
2317 incorrect or missing personalization identifier.

2318 It is important to note that using a Subscriber's name (first or last) as the only method of
2319 personalization is a relatively weak method to thwart a phishing attack since it is fairly easy for an
2320 Attacker to gain this type of information and display it in an email or display it after logging into a
2321 site. Information of a non-public nature is a better candidate for use during personalization.

2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323

2324

2325 **8.3. Authentication Process Assurance Levels**

2326 The stipulations for authentication process assurance levels are described in the following sections.

2327 **8.3.1. Threat Resistance per Assurance Level**

2328 Authentication process assurance levels can be defined in terms of required threat resistance. Table 11 lists
 2329 the threat resistance requirements per assurance level:

2330 Table 11 – Required Authentication Protocol Threat Resistance per Assurance Level

Authentication Process Attacks/Threats	Threat Resistance Requirements			
	Level 1	Level 2	Level 3	Level 4
Online guessing	Yes	Yes	Yes	Yes
Replay	Yes	Yes	Yes	Yes
Session hijacking	No	Yes	Yes	Yes
Eavesdropping	No	Yes	Yes	Yes
Phishing/pharming(verifier impersonation)	No	No	Yes ³¹	Yes
Man in the middle	No	Weak	Weak	Strong
Denial of service/flooding ³²	No	No	No	No

2331
 2332

[KI-IAF: See details below]

2333 **8.3.2. Requirements per Assurance Level**

2334 This section states the requirements levied on the authentication process to achieve the required threat
 2335 resistance at each assurance level.

2336 At Levels 2 and above, the authentication process shall provide sufficient information to the Verifier to
 2337 uniquely identify the appropriate registration information that was (i) provided by the Subscriber at the time
 2338 of registration, and (ii) verified by the RA in the issuance of the token and credential. It is important to note
 2339 that the requirements listed below will not protect the authentication process if malicious code is introduced
 2340 on the Claimant’s machine or at the Verifier.

2341 *[KI-IAF: despite the explicit reference to ‘Level 2 and above...’ this clause is ignored for*
 2342 *mapping purposes, since explicit requirements follow.]*

2343 **8.3.2.1. Level 1**

2344 **8.3.2.1.1** Although there is no identity proofing requirement at this level, the authentication mechanism
 2345 provides some assurance that the same Claimant who participated in previous transactions is accessing the
 2346 protected transaction or data. It allows a wide range of available authentication technologies to be employed
 2347 and permits the use of any of the token methods of Levels 2, 3 or 4.

2348 *[KI-IAF: Tutorial/Implicit]*

2349 **8.3.2.1.2** Successful authentication requires that the Claimant prove, through a secure authentication
 2350 protocol, that he or she possesses and controls the token.

2351 *[KI-IAF: ALI_CM_ASS#030]*

³¹ Long term authentication secrets shall be protected at this level. Short term secrets may or may not be protected.

³² Although there are techniques used to resist flood attacks, no protocol has comprehensive resistance to stop flooding.

2352 8.3.2.1.3 Plaintext passwords or secrets shall not be transmitted across a network at Level 1. However this
2353 level does not require cryptographic methods that block offline analysis by eavesdroppers.
2354 [KI-IAF: AL1_CO_SCO#020]

2355 For example, password challenge-response protocols that combine a password with a challenge to generate
2356 an authentication reply satisfy this requirement although an eavesdropper who intercepts the challenge and
2357 reply may be able to conduct a successful off-line dictionary or password exhaustion attack and recover the
2358 password. Since an eavesdropper who intercepts such a protocol exchange will often be able to find the
2359 password with a straightforward dictionary attack, and this vulnerability is independent of the strength of the
2360 operations, there is no requirement at this level to use Approved cryptographic techniques. At Level 1, long-
2361 term shared authentication secrets may be revealed to Verifiers.
2362 [KI-IAF: Tutorial]

2363 8.3.2.1.4 A wide variety of technologies should be able to meet the requirements of Level 1. For example,
2364 a Verifier might obtain a Subscriber password from a CSP and authenticate the Claimant by use of a
2365 challenge-response protocol. A password sent through a TLS protocol session is another example. Other
2366 common protocols that meet Level 1 requirements include APOP [RFC 1939], S/KEY [RFC 1760], and
2367 password-based versions of Kerberos [KERB].
2368 [KI-IAF: Tutorial]

2369 8.3.2.2. Level 2

2370 8.3.2.2.1 Level 2 allows a wide range of available authentication technologies to be employed and permits
2371 the use of any of the token methods of Levels 2, 3 and 4.
2372 [KI-IAF: Implicit]

2373 8.3.2.2.2 Successful authentication requires that the Claimant shall prove, through a secure authentication
2374 protocol, that he or she controls the token.
2375 [KI-IAF: AL2_CM_ASS#030]

2376 8.3.2.2.3 Session hijacking (when required based on the FIPS 199 security category of the systems as
2377 described below), replay, and online guessing attacks shall be resisted.
2378 [KI-IAF: AL2_CM_CTR#020 a, b, f) - AL2_CO_ISM#030 & AL2_CO_OPN#010 also apply in terms of determining the
2379 categorization – each +NIST SP 800-63-2 Profiling]

2380 8.3.2.2.4 Approved cryptography is required to resist eavesdropping to capture authentication data.
2381 [KI-IAF: AL2_CM_CTR#020 c) - it is assumed that ‘Approved cryptography’ is what meets the SAC requirement that it be shown
2382 to be impractical.]

2383 8.3.2.2.5 Protocols used at Level 2 and above shall be at least weakly man-in-the-middle resistant, as
2384 described in the threat mitigation strategies subsection.
2385 [KI-IAF: AL2_CM_CTR#020 e)]

2386 8.3.2.2.6 Session data transmitted between the Claimant and the RP following a successful Level 2
2387 authentication shall be protected as described in the NIST FISMA guidelines.
2388 [KI-IAF: AL2_CM_ASS#010 +NIST SP 800-63-2 Profiling]

2389 8.3.2.2.7 Specifically, all session data exchanged between information systems that are categorized as
2390 FIPS 199 “Moderate” or “High” for confidentiality and integrity, shall be protected in accordance with NIST
2391 SP 800-53 Control SC-8 (which requires transmission confidentiality) and SC-9 (which requires transmission
2392 integrity).
2393 [KI-IAF: AL2_CM_ASS#010 - AL2_CO_ISM#030 & AL2_CO_OPN#010 also apply in terms of determining the categorization –
2394 each +NIST SP 800-63-2 Profiling]

- 2395 8.3.2.2.8 A wide variety of technologies can meet the requirements of Level 2. For example, a Verifier
2396 might authenticate a Claimant who provides a password through a secure (encrypted) TLS protocol session
2397 (tunneling).
2398 [KI-IAF: AL3_CM_CTR#025 a)]
- 2399 8.3.2.3. Level 3
- 2400 8.3.2.3.1 Level 3 provides multi-factor remote network authentication. At least two authentication factors
2401 are required.
2402 [KI-IAF: AL3_CM_MFA#010]
- 2403 8.3.2.3.2 Level 3 authentication is based on proof of possession of the allowed types of tokens through a
2404 cryptographic protocol. Level 3 also permits any of the token methods of Level 4. Refer to Section 6 for
2405 requirements for single tokens and token combinations that can achieve Level 3 authentication assurance.
2406 [KI-IAF: AL3_CM_ASS#030]
- 2407 8.3.2.3.3 Additionally, at Level 3, strong cryptographic mechanisms shall be used to protect token secret(s)
2408 and authenticator(s).
2409 [KI-IAF: AL3_CO_SCO#010, AL3_CO_SCO 015]
- 2410 8.3.2.3.4 Long-term shared authentication secrets, if used, shall never be revealed to any party except the
2411 Claimant and CSP; .
2412 [KI-IAF: AL3_CO_SCO#020 a, c)]
- 2413 8.3.2.3.5 however, session (temporary) shared secrets may be provided to Verifiers by the CSP, possibly
2414 via the Claimant.
2415 [KI-IAF: AL3_CM_CTR#020 a)]
- 2416 8.3.2.3.6 Approved cryptographic techniques shall be used for all operations including the transfer of
2417 session data.
2418 [KI-IAF: AL3_CO_SCO#010]
- 2419 8.3.2.3.7 Level 3 assurance may be satisfied by client-authenticated TLS (implemented in all modern
2420 browsers), with Claimants who have public key certificates. Other protocols with similar properties may also
2421 be used.
2422 [KI-IAF: Tutorial]
- 2423 8.3.2.3.8 Level 3 authentication assurance may also be met by tunneling the output of a MF OTP Token, or
2424 the output of a SF OTP Token in combination with a Level 2 personal password, through a TLS session.
2425 [KI-IAF: AL3_CM_CTR#025 a)]
- 2426 8.3.2.4. Level 4
- 2427 8.3.2.4.1 Level 4 is intended to provide the highest practical remote network authentication assurance.
2428 Refer to Section 6 for single tokens and token combinations that are allowed to be used to achieve Level 4
2429 authentication assurance.
2430 [KI-IAF: Refer to §6.3.1.1 (single) and §6.3.1.2 (multi-token) mappings – otherwise tutorial]
- 2431 8.3.2.4.2 Level 4 requires strong cryptographic authentication of all parties, and all sensitive data transfers
2432 between the parties. Either public key or symmetric key technology may be used.
2433 [KI-IAF: AL4_CO_SCO#010, AL4_CO_SCO#020, AL4_ID_IDC#010, AL4_ID_IDC#020, AL4_CM_CTR#030,
2434 AL4_CM_IDP#040, AL4_CM_CRN#010 AL4_CM_RVP#020, AL4_CM_RVP #030, AL4_CM_RVP #040,
2435 AL4_CM_RV P#050, AL4_CM_RKY#010, AL4_CM_CSM#020, AL4_CM_CSM #030, AL4_CM_CSM #040,
2436 AL4_CM_ASS#010]

- 2437 8.3.2.4.3 The token secret shall be protected from compromise through the malicious code threat as
2438 described in Section 8.1.3 above.
2439 [KI-IAF: AL4_CM_CTR#030 a)]
- 2440 8.3.2.4.4 Long-term shared authentication secrets, if used, shall never be revealed to any party except the
2441 Claimant and CSP; however session (temporary) shared secrets may be provided to Verifiers or RPs by the
2442 CSP.
- 2443 8.3.2.4.5 Strong, approved cryptographic techniques shall be used for all operations including the transfer
2444 of session data.
2445 [KI-IAF: AL4_CO_SCO#010]
- 2446 8.3.2.4.6 All sensitive data transfers shall be cryptographically authenticated using keys that are derived
2447 from the authentication process in such a way that MitM attacks are strongly resisted.
2448 [KI-IAF: AL4_CM_CTR#020 e)]
- 2449 8.3.2.4.7 Level 4 assurance may be satisfied by client-authenticated TLS (implemented in all modern
2450 browsers), with Claimants who have public key MF Hardware Cryptographic Tokens. Other protocols with
2451 similar properties can also be used.
2452 [KI-IAF: Tutorial]
- 2453 8.3.2.4.8 It should be noted that, in multi-token schemes, the token used to provide strong man-in-the-
2454 middle resistance need not be a hardware token.
2455 [KI-IAF: AL4_CM_CRN#075, AL4_CM_MFA#010]
- 2456 For example, if a software cryptographic token is used to open a client-authenticated TLS session, and the
2457 output of a multifactor OTP device is sent by the claimant in that session, then the resultant protocol will still
2458 provide Level 4 assurance.
2459 [KI-IAF: Tutorial]
- 2460

2461 9. Assertions

2462 9.1. Overview

2463 Assertions are statements from a Verifier to an RP that contain information about a Subscriber. Assertions
2464 are used when the RP and the Verifier are not collocated (i.e., they are connected through a shared network).
2465 The RP uses the information in the assertion to identify the Claimant and make authorization decisions about
2466 his or her access to resources controlled by the RP. An assertion may include identification and
2467 authentication statements regarding the Subscriber, and may additionally include attribute statements that
2468 further characterize the Subscriber and support the authorization decision at the RP.

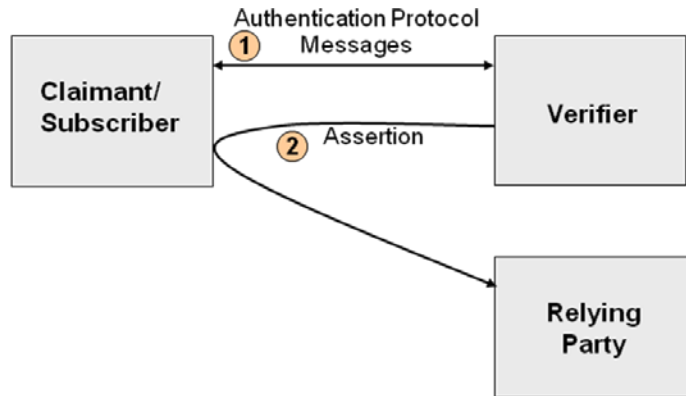
2469 Assertion-based authentication of the Claimant serves several important goals. It supports the process of
2470 Single-Sign-On for Claimants, allowing them to authenticate once to a Verifier and subsequently obtain
2471 services from multiple RPs without being aware of further authentication. Assertion mechanisms also support
2472 the implementation of a federated identity for a Subscriber, allowing the linkage of multiple
2473 identities/accounts held by the Subscriber with different RPs through the use of a common “federated”
2474 identifier. In this context, a federation is a group of entities (RPs, Verifiers and CSPs) that are bound together
2475 through common agreed-upon business practices, policies, trust mechanisms, profiles and protocols. Finally,
2476 assertion mechanisms can also facilitate authentication schemes that are based on the attributes or
2477 characteristics of the Claimant in lieu of (or in addition to) the identity of the Claimant. Attributes are often
2478 used in determining access privileges for Attributes Based Access Control (ABAC) or Role Based Access
2479 Control (RBAC).

2480 It is important to note that assertion schemes are fairly complex multiparty protocols, and therefore have
2481 fairly subtle security requirements which shall be satisfied. When evaluating a particular assertion scheme, it
2482 may be instructive to break it down into its component interactions. Generally speaking, interactions between
2483 the Claimant/Subscriber and the Verifier and between the Claimant/Subscriber and RP are similar to the
2484 authentication mechanisms presented in Section 8, while interactions between the Verifier and RP are similar
2485 to the *token and credential verification services* presented in Section 7. Many of the requirements presented
2486 in this section will, therefore, be similar to corresponding requirements in those two sections.

2487 There are two basic models for assertion-based authentication. After successful authentication with the
2488 Verifier, the Subscriber is issued an assertion or an assertion reference, which the Subscriber uses to
2489 authenticate to the RP.

2490 a) *The Direct Model* – In the direct model, the Claimant ~~use~~ offers to the Verifier his or her e-
2491 authentication token ~~to authenticate to the Verifier~~. Following the Verifier’s successful
2492 authentication of the Claimant, the Verifier creates an assertion, and sends it to the Subscriber
2493 to be forwarded to the RP. The assertion is used by the Claimant/Subscriber to enable the RP
2494 to authenticate them ~~the RP~~. (This is usually handled automatically by the Subscriber’s
2495 browser.) Figure 4 illustrates this model.

2496



2497

2498

2499 Figure 4 - Direct Assertion Model

2500

2501

2502

2503

2504

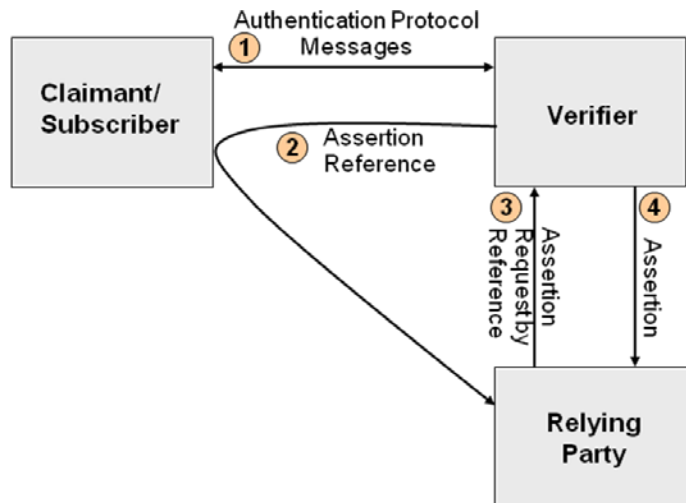
2505

2506

2507

2508

- b) *The Indirect Model* – In the indirect model, the Claimant ~~use~~offers his or her token ~~to~~ **authenticate** to the Verifier. Following successful authentication, the Verifier creates an assertion as well as an assertion reference (which identifies the Verifier and includes a pointer to the full assertion held by the Verifier). The assertion reference is sent to the Subscriber to be forwarded to the RP. In this model, the assertion reference is used by the Claimant/Subscriber **in order to be authenticated by** ~~to~~ the RP. The RP then uses the assertion reference to explicitly request the assertion from the Verifier. Figure 5 illustrates this model.



2509

2510

2511 Figure 5 - Indirect Assertion Model

2512

2513

2514

2515

As mentioned earlier, an assertion contains a set of claims or statements about an authenticated Subscriber. Based on the statements contained within it, an authentication assertion will fall into one of two categories (and either category can be used in both direct and indirect models):

2516

2517

2518

- a) *Holder-of-Key Assertions* – A holder-of-key assertion contains a reference to a symmetric key or a public key (corresponding to a private key) possessed by the Subscriber. The RP may require the Subscriber to prove possession of the secret that is referenced in the assertion. In

2519 proving possession of the Subscriber’s secret, the Subscriber also proves with a certain degree
2520 of assurance that he or she is the rightful owner of the assertion. It is therefore difficult for an
2521 Attacker to use a holder-of-key assertion issued to a Subscriber, since the former cannot prove
2522 possession of the secret referenced within the assertion.

2523 b) *Bearer Assertions* – A bearer assertion does not provide a mechanism for the Claimant to
2524 prove that he or she is the rightful owner of the assertion. The RP has to assume that the
2525 assertion was issued to the Subscriber who presents the assertion or the corresponding
2526 assertion reference to the RP. If a bearer assertion (in the direct model) or assertion reference
2527 (in the indirect model) belonging to a Subscriber is captured, copied, or manufactured by an
2528 Attacker, the latter can impersonate the rightful Subscriber to obtain services from the RP.
2529 Bearer assertions can be made secure only if some part of the assertion or assertion reference,
2530 sent to the Subscriber by the Verifier, is unpredictable to an Attacker and can reliably be kept
2531 secret.

2532

2533 There are cases in which the RP should be anonymous to the Verifier for the purpose of privacy. The direct
2534 model is more suitable for the “anonymous RP” scenario since there is no requirement for the RP to
2535 authenticate to the Verifier as in the indirect model. However, it is possible to devise authentication schemes
2536 (e.g., using key hierarchies within a group or federation) that allow the use of the indirect model to support
2537 the “anonymous RP” scenario.

2538 There are other cases where privacy concerns require that the Claimant’s identity/account at the Verifier and
2539 RP not be linked through use of a common identifier/account name. In such scenarios, pseudonymous
2540 identifiers are used within the assertions generated by the Verifier for the RP.

2541 It should be noted that the two models described above are abstractions. There may be other interactions
2542 between the three players preceding or interspersed with the interactions described in the model. For
2543 example, the Claimant may initiate a connection with an RP of his or her choice, at which point, the latter
2544 would redirect the Claimant to an appropriate Verifier to be authenticated using the direct model, resulting in
2545 an assertion being sent to the RP. Alternately, the Claimant may first authenticate to a Verifier of his or her
2546 choice and then select one or more RPs to obtain further services. The direct model is used to generate
2547 assertions for each of these RPs. Parallel scenarios may be constructed for the indirect model as well.

2548 There is one other basic assertion model, *The Proxy Model*. In the proxy model, the Claimant
2549 uses his or her e-authentication token to authenticate to the Verifier. Following successful
2550 authentication of the Claimant, the Verifier creates an assertion and includes it when
2551 interacting directly with the RP, acting as an intermediary between the Claimant and the RP.
2552 Figure 6 illustrates this model.

2553
2554



2555
2556
2557
2558
2559

Figure 6 – Proxy Model

2560 The RP grants or denies the request based, at least in part, on the authentication
2561 assertion made by the Verifier. There are several common reasons for such proxies:

- 2562
- 2563 a) Portals that provide users access to multiple RPs that require user
2564 authentication
- 2565 b) Web caching mechanisms that are required to satisfy the RP's access control
2566 policies, especially when client-authenticated TLS with the Claimant is
2567 required
- 2568 c) Network monitoring and/or filtering mechanisms that terminate TLS in order to
2569 inspect and manipulate the traffic

2570

2571 It is good practice to protect communications between the Verifier and the RP.
2572 Current commercial implementations tend to do this by having the proxy use client-
2573 authenticated TLS with the Verifier and pass the authentication assertion in the HTTP
2574 header.

2575

2576 Note that the Verifier may have access to information that may be useful to the RP in
2577 enforcing security policies, such as device identity, location, system health checks, and
2578 configuration management. If so, it may be a good idea to pass this information along
2579 to the RP.

2580

2581 Three types of assertion technologies will be discussed within this section: Web browser cookies, SAML
2582 (Security Assertion Markup Language) assertions, and Kerberos tickets. Other assertion technologies may be
2583 used in an e-authentication environment as long as they meet the requirements set forth in Section 9.3 below
2584 for the targeted assurance level.

2585 **9.1.1. Cookies**

2586 One type of assertion widely in use is Web cookie technology. Cookies are text files used by a browser to
2587 store information provided by a particular web site. The contents of the cookie are sent back to the web site
2588 each time the browser requests a page from the same web site. The web site uses the contents of the cookie to
2589 identify the user and prepare customized Web pages for that user, or to authorize the user for certain
2590 transactions.

2591 Cookies have two mandatory parameters:

- 2592 a) *Name* – This parameter states the name of the cookie.
- 2593 b) *Value* – This parameter holds information that a cookie is storing. For example, the value
2594 parameter could hold a user ID or session ID.

2595 Cookies also have four optional parameters:

- 2596 a) *Expiration date* – This parameter determines how long the cookie stays valid.
- 2597 b) *Path* – This parameter sets the path over which the cookie is valid.
- 2598 c) *Domain* – This parameter determines the domain in which the cookie is valid.
- 2599 d) *Secure* – This parameter indicates the cookie requires that a secure connection exist for the
2600 cookie to be used.

2601 There are two types of cookies:

- 2602 a) *Session cookies* – A cookie that is erased when the user closes the web browser. The session
2603 cookie is stored in temporary memory and is not retained after the browser is closed.
- 2604 b) *Persistent cookies* – A cookie that is stored on a user’s hard drive until it expires (persistent
2605 cookies are set with expiration dates) or until the user deletes the cookie.

2606 Cookies are effective as assertions for Internet single-sign-on where the RP and Verifier are part of the same
2607 Internet domain, and when the cookie contains authentication status for that domain. They are not usable in
2608 scenarios where the RP and the Verifier are part of disparate domains.

2609 Cookies are also often used by the Claimant to re-authenticate to a server. This may be considered to be a use
2610 of assertion technology. In this case, the server acts as a Verifier when it sets the cookie in the Subscriber’s
2611 browser, and as an RP when it requests the cookie from a Claimant who wishes to re-authenticate to it. Often,
2612 the cookie contains a random number, and the assertion data that it represents does not leave the server. Note
2613 that, if the cookie is used as an assertion reference in this way, no assertion needs to be sent on an open
2614 network, and therefore, confidentiality and integrity requirements for assertion data at Level 2 and below
2615 may be satisfied by access controls rather than by cryptographic methods. (The cookie itself, however, does
2616 need to be protected.) This is in line with the credential storage requirement presented in Section 7.

2617 **9.1.2. Security Assertion Markup Language (SAML) Assertions**

2618 SAML is an XML-based framework for creating and exchanging authentication and attribute information
2619 between trusted entities over the Internet. As of this writing, the latest specification for [[SAML](#)] is SAML
2620 v2.0, issued 15 March 2005.

2621 The building blocks of SAML include the Assertions XML schema which define the structure of the
2622 assertion; the SAML Protocols which are used to request assertions and artifacts (that is, the assertion
2623 reference mentioned in Section 9.1); and the Bindings that define the underlying communication protocols
2624 (such as HTTP or SOAP) and that can be used to transport the SAML assertions. The three components
2625 above define a SAML profile that corresponds to a particular use case such as “Web Browser SSO”.

2626 SAML Assertions are encoded in an XML schema and can carry up to three types of statements:

- 2627 a) *Authentication statements* – Include information about the assertion issuer, the authenticated
2628 subject, validity period, and other authentication information. For example, an Authentication
2629 Assertion would state the subject “John” was authenticated using a password at 10:32pm on
2630 06-06-2004.
- 2631 b) *Attribute statements* – Contain specific additional characteristics related to the Subscriber. For
2632 example, subject “John” is associated with attribute “Role” with value “Manager”.
- 2633 c) *Authorization statements* – Identify the resources the Subscriber has permission to access.
2634 These resources may include specific devices, files, and information on specific web servers.
2635 For example, subject “John” for action “Read” on “Webserver1002” given evidence “Role”.

2636 Authorization statements are beyond the scope of this document and will not be discussed.

2637 **9.1.3. Kerberos Tickets**

2638 The Kerberos Network Authentication Service [[RFC 4120](#)] was designed to provide strong authentication for
2639 client/server applications using symmetric-key cryptography. Extensions to Kerberos can support the use of
2640 public key cryptography for selected steps of the protocol. Kerberos also supports confidentiality and
2641 integrity protection of session data between the Subscriber and the RP.

2642 Kerberos supports authentication of a Claimant over an untrusted, shared network using two or more
2643 Verifiers. The Claimant implicitly authenticates to the Verifier by demonstrating the ability to decrypt a
2644 random session key encrypted for the Subscriber by the Verifier. (Some Kerberos variants also require the
2645 Subscriber to explicitly authenticate to the Verifier, but this is not universal.) In addition to the encrypted
2646 session key, the Verifier also generates another encrypted object called a Kerberos ticket. The ticket contains
2647 the same session key, the identity of the Subscriber to whom the session key was issued, and an expiration
2648 time after which the session key is no longer valid. The ticket is confidentiality and integrity protected by a
2649 pre-established that is key shared between the Verifier and the RP.

2650 To authenticate using the session key, the Claimant sends the ticket to the RP along with encrypted data that
2651 proves that the Claimant possesses the session key embedded within the Kerberos ticket. Session keys are
2652 either used to generate new tickets, or to encrypt and authenticate communications between the Subscriber
2653 and the RP.

2654 To begin the process, the Claimant sends an authentication request to the Authentication Server (AS). The
2655 AS encrypts a session key for the Subscriber using the Subscriber's long term credential. The long term
2656 credential may either be a secret key shared between the AS and the Subscriber, or in the PKINIT variant of
2657 Kerberos, a public key certificate. It should be noted that most variants of Kerberos based on a shared secret
2658 key between the Subscriber and Verifier derive this key from a user generated password. As such, they are
2659 vulnerable to offline dictionary attack by a passive eavesdropper.

2660 In addition to delivering the session key to the subscriber, the AS also issues a ticket using a key it shares
2661 with the Ticket Granting Server (TGS). This ticket is referred to as a Ticket Granting Ticket (TGT), since the
2662 verifier uses the session key in the TGT to issue tickets rather than to explicitly authenticate the Claimant.
2663 The TGS uses the session key in the TGT to encrypt a new session key for the Subscriber and uses a key it
2664 shares with the RP to generate a ticket corresponding to the new session key. The subscriber decrypts the
2665 session key and uses the ticket and the new session key together to authenticate to the RP.

2666 **9.2. Assertion Threats**

2667 In this section, it is assumed that the two endpoints of the assertion transmission (namely, the Verifier and the
2668 RP) are uncompromised. However, the Claimant is not assumed to be entirely trustworthy as the Claimant
2669 may have an interest in modifying or replacing an assertion to obtain a greater level of access to a
2670 resource/service provided by the RP. Other Attackers are assumed to lurk within the shared transmission
2671 medium (e.g., Internet) and may be interested in obtaining or modifying assertions and assertion references to
2672 impersonate a Subscriber or access unauthorized data or services. Furthermore, it is possible that two or more
2673 entities may be colluding to attack another party. An Attacker may attempt to subvert assertion protocols by
2674 directly compromising the integrity or confidentiality of the assertion data. For the purpose of this type of
2675 threat, authorized parties who attempt to exceed their privileges may be considered Attackers.

2676 a) *Assertion manufacture/modification* – An Attacker may generate a bogus assertion or modify
2677 the assertion content (such as the authentication or attribute statements) of an existing
2678 assertion, causing the RP to grant inappropriate access to the Subscriber. For example, an
2679 Attacker may modify the assertion to extend the validity period; a Subscriber may modify the
2680 assertion to have access to information that they should not be able to view.

2681 b) *Assertion disclosure* – Assertions may contain authentication and attribute statements that
2682 include sensitive Subscriber information. Disclosure of the assertion contents can make the
2683 Subscriber vulnerable to other types of attacks.

- 2684 c) *Assertion repudiation by the Verifier* – An assertion may be repudiated by a Verifier if the
2685 proper mechanisms are not in place. For example, if a Verifier does not digitally sign an
2686 assertion, the Verifier can claim that it was not generated through the services of the Verifier.
- 2687 d) *Assertion repudiation by the Subscriber* – Since it is possible for a compromised or malicious
2688 subscriber to issue assertions to the wrong party, a subscriber can repudiate any transaction
2689 with the RP that was authenticated using only a bearer assertion.
- 2690 e) *Assertion redirect*: An Attacker uses the assertion generated for one RP to obtain access to a
2691 second RP.
- 2692 f) *Assertion reuse* – An Attacker attempts to use an assertion that has already been used once
2693 with the intended RP.

2694 In addition to reliable and confidential transmission of assertion data from the Verifier to the RP, assertion
2695 protocols have a further goal: in order for the Subscriber to be recognized by the RP, he or she shall be
2696 issued some secret information, the knowledge of which distinguishes the Subscriber from Attackers who
2697 wish to impersonate the Subscriber. In the case of holder-of-key assertions, this secret is generally the
2698 Subscriber's long term token secret, which would already have been established with the CSP prior to the
2699 initiation of the assertion protocol.³³

2700 In other cases, however, the Verifier will generate a temporary secret and transmit it to the authenticated
2701 Subscriber for this purpose. Since, when this secret is used to authenticate to the RP, it generally replaces the
2702 token authenticator in the type of protocols described in Section 8, this temporary secret will be referred to
2703 here as a secondary authenticator. Secondary authenticators include assertions in the direct model, session
2704 keys in Kerberos, assertion references in the indirect model, and cookies used for authentication. The threats
2705 to the secondary authenticator are as follows:

- 2706 a) *Secondary authenticator manufacture* – An Attacker may attempt to generate a valid
2707 secondary authenticator and use it to impersonate a Subscriber.
- 2708 b) *Secondary authenticator capture* – The Attacker may use a session hijacking attack to capture
2709 the secondary authenticator when the Verifier transmits it to the Subscriber after the primary
2710 authentication step, or the Attacker may use a man-in-the-middle attack to obtain the
2711 secondary authenticator as it is being used by the Subscriber to authenticate to the RP. If, as in
2712 the indirect model, the RP needs to send the secondary authenticator back to the Verifier in
2713 order to check its validity or obtain the corresponding assertion data, an Attacker may
2714 similarly subvert the communication protocol between the Verifier and the RP to capture a
2715 secondary authenticator. In any of the above scenarios, the secondary authenticator can be
2716 used to impersonate the Subscriber.

2717

2718 Finally, in order for the Subscriber's authentication to the RP to be useful, the binding between the secret
2719 used to authenticate to the RP and the assertion data referring to the Subscriber shall be strong.

- 2720 a) *Assertion substitution* – A subscriber may attempt to impersonate a more privileged subscriber
2721 by subverting the communication channel between the Verifier and RP, for example by
2722 reordering the messages, to convince the RP that his or her secondary authenticator

³³ The role of the Verifier in such protocols is not necessarily to issue new secrets. Rather, in a holder-of-key-assertion, the Verifier communicates the information in the Subscriber's credential (as well as any supplementary information from the CSP such as revocation data) to the RP. The Verifier also vouches that the holder-of-key assertion represents current information from a trusted source (the CSP.)

2723 corresponds to assertion data sent on behalf of the more privileged subscriber. This is
2724 primarily a threat to the indirect model, since in the direct model, assertion data is directly
2725 encoded in the secondary authenticator.

2726 **9.2.1. Threat Mitigation Strategies**

2727 Mitigation techniques are described below for each of the threats described in the last subsection.

2728 Logically speaking, an assertion is issued by a Verifier and consumed by an RP – these are the two end
2729 points of the session that needs to be secured to protect the assertion. In the direct model, the session in
2730 which the assertion is passed traverses the Subscriber. Furthermore, in the current web environment, the
2731 assertion may pass through two separate secure sessions (one between the Verifier and the Subscriber, and
2732 the other between the Subscriber and the RP), with a break in session security on the Subscriber’s browser.
2733 This is reflected in the mitigation strategies described below. In the indirect model, the assertion flows
2734 directly from the Verifier to the RP; this protocol session needs to be protected. All of the threat mitigation
2735 strategies in Section 8 apply to the protocols used to request, retrieve and submit assertions and assertion
2736 references.

2737 a) *Assertion manufacture/modification*: To mitigate this threat, one of the following mechanisms
2738 may be used:

2739 i) The assertion may be digitally signed by the Verifier. The RP should check the digital
2740 signature to verify that it was issued by a legitimate Verifier.

2741 ii) The assertion may be sent over a protected session such as TLS/SSL. In order to protect
2742 the integrity of assertions from malicious attack, the Verifier shall be authenticated.

2743 b) *Assertion disclosure* – To mitigate this threat, one of the following mechanisms may be
2744 implemented:

2745 i) The assertion may be sent over a protected session to an authenticated RP. Note that, in
2746 order to protect assertions against both disclosure and manufacture/modification using a
2747 protected session, both the RP and the Verifier need to be authenticated.

2748 ii) If assertions are signed by the Verifier, they may be encrypted for a specific RP with no
2749 additional integrity protection. It should be noted that any protocol that requires a series of
2750 messages between two parties to be signed by their source and encrypted for their
2751 recipient provides all the same guarantees as a mutually authenticated protected session,
2752 and may therefore be considered equivalent. The general requirement for protecting
2753 against both assertion disclosure and assertion manufacture/modification may therefore be
2754 described as a mutually authenticated protected session or equivalent between Verifier and
2755 RP.

2756 c) *Assertion repudiation by the Verifier* – To mitigate this threat, the assertion may be digitally
2757 signed by the Verifier using a key that supports non-repudiation. The RP should check the
2758 digital signature to verify that it was issued by a legitimate Verifier.

2759 d) *Assertion repudiation by the Subscriber* – To mitigate this threat, the Verifier may issue
2760 holder of key, rather than bearer assertions. The Subscriber can then prove possession of the
2761 asserted key to the RP. If the asserted key matches the subscriber’s long term credential (as
2762 provided by the CSP) it will be clear to all parties involved that it was the Subscriber who
2763 authenticated to the RP rather than a compromised Verifier impersonating the Subscriber.

- 2764 e) *Assertion redirect* – To mitigate this threat, the assertion may include the identity of the RP
2765 for whom it was generated. The RP verifies that incoming assertions include its identity as the
2766 recipient of the assertion.
- 2767 f) *Assertion reuse* – To mitigate this threat, the following mechanisms may be used:
- 2768 i) The assertion includes a timestamp and has a short lifetime of validity. The RP checks the
2769 timestamp and lifetime values to ensure that the assertion is currently valid. The lifetime
2770 value may either be in the assertion or set by the RP.
- 2771 ii) The RP keeps track of assertions that were consumed within a (configurable) time window
2772 to ensure that an assertion cannot be used more than once within that time window.
- 2773 g) *Secondary authenticator manufacture* – To mitigate this threat, one of the following
2774 mechanisms may be implemented:
- 2775 i) The secondary authenticator may contain sufficient entropy that an Attacker without direct
2776 access to the Verifier’s random number generator cannot guess the value of a valid
2777 secondary authenticator.
- 2778 ii) The secondary authenticator may contain timely assertion data that is signed by the
2779 Verifier or integrity protected using a key shared between the Verifier and the RP.
- 2780 iii) The Subscriber may authenticate to the RP directly using his or her long term token and
2781 avoid the need for a secondary authenticator altogether.
- 2782 h) *Secondary authenticator capture* – To mitigate this threat, adequate protections shall be in
2783 place throughout the lifetime of any secondary authenticators used in the assertion protocol.
- 2784 i) In order to protect the secondary authenticator while it is in transit between the Verifier
2785 and the Subscriber, the secondary authenticator shall be sent via a protected session
2786 established during the primary authentication of the Subscriber using his or her token. This
2787 requirement is the same as the requirement in Section 8, regarding the Authentication
2788 Process, to protect sensitive data (in this case the secondary authenticator) from session
2789 hijacking attacks.
- 2790 ii) In order to protect the secondary authenticator from capture as it is submitted to the RP,
2791 the secondary authenticator shall be used in an authentication protocol which protects
2792 against eavesdropping and man-in-the-middle attacks as described in Section 8.
- 2793 iii) In order to protect the secondary authenticator after it has been used, it shall never be
2794 transmitted on an unprotected session or to an unauthenticated party while it is still valid.
2795 The secondary authenticator may be sent in the clear only if the sending party has strong
2796 assurances that the secondary authenticator will not subsequently be accepted by any other
2797 RP. This is possible if the secondary authenticator is specific to a single RP, and if that RP
2798 will not accept secondary authenticators with the same value until the maximum lifespan
2799 of the corresponding assertion has passed.
- 2800 i) *Assertion substitution* – To mitigate this threat, one of the following mechanisms may be
2801 implemented:

- 2802 i) Responses to assertion requests, signed or integrity protected by the Verifier, may contain
 2803 the value of the assertion reference used in the request or some other nonce that was
 2804 cryptographically bound to the request by the RP.
- 2805 ii) Responses to assertion requests may be bound to the corresponding requests by message
 2806 order, as in HTTP, provided that assertions and requests are protected by a protocol such
 2807 as TLS that can detect and disallow malicious reordering of packets.

2808 **9.3. Assertion Assurance Levels**

2809 The stipulations for assertion assurance levels are described in the next sections.

2810 **9.3.1. Threat Resistance per Assurance Level**

2811 Table 12 lists the requirements for assertions (both in the direct and indirect models) and assertion references
 2812 (in the indirect model) at each assurance level in terms of resistance to the threats listed above.

2813 Table 12 – Threat Resistance per Assurance Level

Threat	Level 1	Level 2	Level 3	Level 4
Assertion manufacture/modification	Yes	Yes	Yes	Yes
Assertion disclosure	No	Yes	Yes	Yes
Assertion repudiation by Verifier	No	No	Yes ³⁴	Yes ³⁴
Assertion repudiation by Subscriber	No	No	No	Yes ³⁴
Assertion redirect	No	Yes	Yes	Yes
Assertion reuse	Yes	Yes	Yes	Yes
Secondary authenticator manufacture	Yes	Yes	Yes	Yes
Secondary authenticator capture	No	Yes	Yes	Yes
Assertion substitution	No	Yes	Yes	Yes

2814
 2815 [KI-IAF: See details below]

2816 **9.3.2. Requirements per Assurance Level**

2817 The following sections summarize the requirements for assertions at each assurance level.

2818 **9.3.2.0.1** All assertions recognized within this guideline shall indicate the assurance level of the initial
 2819 authentication of the Claimant to the Verifier. The assurance level indication within the assertion may be
 2820 implicit (e.g., through the identity of the Verifier implicitly indicating the resulting assurance level) or
 2821 explicit (e.g., through an explicit field within the assertion).

2822 [KI-IAF: AL1/2/3/4_CM_VAS#030]

2823 **9.3.2.1. Level 1**

2824 **9.3.2.1.1** At Level 1, it must be impractical for an Attacker to manufacture an assertion or assertion
 2825 reference that can be used to impersonate the Subscriber.

2826 [KI-IAF: AL1_CM_VAS#060 a, b, c]

³⁴ Except for Kerberos.

- 2827 9.3.2.1.2 If the direct model is used, the assertion which is used shall be signed by the Verifier or integrity-
2828 protected using a secret key shared by the Verifier and RP, and if the indirect model is used, the assertion
2829 reference which is used shall have a minimum of 64 bits of entropy.
2830 [KI-IAF: AL1_CM_VAS#060 a, b, c)]
- 2831 9.3.2.1.3 Bearer assertions shall be specific to a single transaction.³⁵
2832 [KI-IAF: AL1_CM_VAS#080]
- 2833 9.3.2.1.4 Also, if assertion references are used, they shall be freshly-generated whenever a new assertion is
2834 created by the Verifier. In other words, bearer assertions and assertion references are generated for one-time
2835 use.
2836 [KI-IAF: AL1_CM_VAS#090]
- 2837 9.3.2.1.5 Furthermore, in order to protect assertions against modification in the indirect model, all
2838 assertions sent from the Verifier to the RP shall either be signed by the Verifier, or transmitted from an
2839 authenticated Verifier via a protected session.
2840 [KI-IAF: AL1_CM_VAS#060 d)]
- 2841 9.3.2.1.6 In either case, a strong mechanism must be in place which allows the RP to establish a binding
2842 between the assertion reference and its corresponding assertion, based on integrity protected (or signed)
2843 communications with the authenticated Verifier.
2844 [KI-IAF: AL1_CM_VAS#100]
- 2845 9.3.2.1.7 To lessen the impact of captured assertions and assertion references, assertions that are consumed
2846 by an RP which is not part of the same Internet domain as the Verifier shall expire if they are not used within
2847 5 minutes of their creation.
2848 [KI-IAF: AL1_CM_VAS#110 a)]
- 2849 9.3.2.1.8 Assertions intended for use within a single Internet domain, including assertions contained in or
2850 referenced by cookies, however, may last as long as 12 hours without being used.
2851 [KI-IAF: AL1_CM_VAS#110 b)]
- 2852 9.3.2.2. Level 2
- 2853 9.3.2.2.0 All stipulations from Level 1 apply.
2854 [KI-IAF: ... and are re-mapped at AL2 below – Note however, in SP 800-63-2 the above phrase actually appears between text
2855 which is here identified as 9.3.2.2.11 and 9.3.2.2.12. The presents clause is numbered '2.0 to maintain the alignment within this
2856 document in following AL sections.]
- 2857 9.3.2.2.1 At Level 2, it must be impractical for an Attacker to manufacture an assertion or assertion
2858 reference that can be used to impersonate the Subscriber.
2859 [KI-IAF: AL2_CM_VAS#060 a, b, c)]
- 2860 9.3.2.2.2 If the direct model is used, the assertion which is used shall be signed by the Verifier or integrity-
2861 protected using a secret key shared by the Verifier and RP, and if the indirect model is used, the assertion
2862 reference which is used shall have a minimum of 64 bits of entropy.
2863 [KI-IAF: AL2_CM_VAS#060 a, b, c)]
- 2864 9.3.2.2.3 Bearer assertions shall be specific to a single transaction.³⁶
2865 [KI-IAF: AL2_CM_VAS#080]

³⁵ For example, implementation of SSO requires a separate assertion each time a new session is started with a participating RP.

³⁶ For example, implementation of SSO requires a separate assertion each time a new session is started with a participating RP.

- 2866 9.3.2.2.4 Also, if assertion references are used, they shall be freshly-generated whenever a new assertion is
2867 created by the Verifier. In other words, bearer assertions and assertion references are generated for one-time
2868 use.
2869 [KI-IAF: AL2_CM_VAS#090]
- 2870 9.3.2.2.5 Furthermore, in order to protect assertions against modification in the indirect model, all
2871 assertions sent from the Verifier to the RP shall either be signed by the Verifier, or transmitted from an
2872 authenticated Verifier via a protected session.
2873 [KI-IAF: AL2_CM_VAS#060 d)]
- 2874 9.3.2.2.6 In either case, a strong mechanism must be in place which allows the RP to establish a binding
2875 between the assertion reference and its corresponding assertion, based on integrity protected (or signed)
2876 communications with the authenticated Verifier.
2877 [KI-IAF: AL2_CM_VAS#100]
- 2878 9.3.2.2.7 To lessen the impact of captured assertions and assertion references, assertions that are consumed
2879 by an RP which is not part of the same Internet domain as the Verifier shall expire if they are not used within
2880 5 minutes of their creation.
2881 [KI-IAF: AL2_CM_VAS#110 a)]
- 2882 9.3.2.2.8 Assertions intended for use within a single Internet domain, including assertions contained in or
2883 referenced by cookies, however, may last as long as 12 hours without being used.
2884 [KI-IAF: AL2_CM_VAS#110 b)]
- 2885 9.3.2.2.9 If the underlying credential specifies that the subscriber name is a pseudonym, this information
2886 must be conveyed in the assertion.
2887 [KI-IAF: AL2_CM_VAS#040]
- 2888 9.3.2.2.10 Level 2 assertions shall be protected against manufacture/modification, capture, redirect and
2889 reuse. Assertion references shall be protected against manufacture, capture and reuse.
2890 [KI-IAF: AL2_CM_VAS#070 a, b)]
- 2891 9.3.2.2.11 Each assertion shall be targeted for a single RP
2892 [KI-IAF: AL2_CM_VAS#050]
- 2893 and the RP shall validate that it is the intended recipient of the incoming assertion.
2894 [KI-IAF: SAC do not apply to RPs, hence no mapping]
- 2895 9.3.2.2.12 Additionally, assertions, assertion references and any session cookies used by the Verifier or RP
2896 for authentication purposes, shall be transmitted to the Subscriber through a protected session which is linked
2897 to the primary authentication process in such a way that session hijacking attacks are resisted (see Section
2898 8.2.2 for methods which may be used to protect against session hijacking attacks).
2899 [KI-IAF: AL2_CM_VAS#070 c)]
- 2900 9.3.2.2.13 Assertions, assertion references and session cookies shall not be subsequently transmitted over an
2901 unprotected session or to an unauthenticated party while they remain valid.
2902 [KI-IAF: AL2_CM_VAS#070 c)]
- 2903 9.3.2.2.14 (To this end, any session cookies used for authentication purposes shall be flagged as secure, and
2904 redirects used to forward secondary authenticators from the Subscriber to the RP shall specify a secure
2905 protocol such as HTTPS.)
2906 [KI-IAF: AL2_CM_VAS#070 c)]

- 2907 9.3.2.2.15 To protect assertions against manufacture, modification, and disclosure, assertions which are sent
2908 from the Verifier to the RP, whether directly or through the Subscriber's device, shall either be sent via a
2909 mutually authenticated protected session between the Verifier and RP, or equivalently shall be signed by the
2910 Verifier and encrypted for the RP.
2911 [KI-IAF: AL2_CM_VAS#060 a & b]
- 2912 9.3.2.2.16 All assertion protocols used at Level 2 and above require the use of Approved cryptographic
2913 techniques.
2914 [KI-IAF: AL2_CM_VAS#010]
- 2915 9.3.2.2.17 As such, the use of Kerberos keys derived from user-generated passwords is not permitted at
2916 Level 2 or above.
2917 [KI-IAF: AL2_CM_VAS#010 +NIST SP 800-63-2 Profiling]
- 2918 9.3.2.3. Level 3
- 2919 9.3.2.3.0 At Level 3, in addition to Level 2 requirements,
2920 [KI-IAF: Which are repeated as '3.1 to '3.17, so as to provide consistent mapping.]
- 2921 9.3.2.3.1 At Level 3, it must be impractical for an Attacker to manufacture an assertion or assertion
2922 reference that can be used to impersonate the Subscriber.
2923 [KI-IAF: AL3_CM_VAS#060 a, b, c)]
- 2924 9.3.2.3.2 If the direct model is used, the assertion which is used shall be signed by the Verifier or integrity-
2925 protected using a secret key shared by the Verifier and RP, and if the indirect model is used, the assertion
2926 reference which is used shall have a minimum of 64 bits of entropy.
2927 [KI-IAF: AL3_CM_VAS#060 a, b, c)]
- 2928 9.3.2.3.3 Bearer assertions shall be specific to a single transaction.³⁷
2929 [KI-IAF: AL3_CM_VAS#080]
- 2930 9.3.2.3.4 Also, if assertion references are used, they shall be freshly-generated whenever a new assertion is
2931 created by the Verifier. In other words, bearer assertions and assertion references are generated for one-time
2932 use.
2933 [KI-IAF: AL3_CM_VAS#090]
- 2934 9.3.2.3.5 Furthermore, in order to protect assertions against modification in the indirect model, all
2935 assertions sent from the Verifier to the RP shall either be signed by the Verifier, or transmitted from an
2936 authenticated Verifier via a protected session.
2937 [KI-IAF: AL3_CM_VAS#060 d)]
- 2938 9.3.2.3.6 In either case, a strong mechanism must be in place which allows the RP to establish a binding
2939 between the assertion reference and its corresponding assertion, based on integrity protected (or signed)
2940 communications with the authenticated Verifier.
2941 [KI-IAF: AL3_CM_VAS#100]
- 2942 9.3.2.3.7 To lessen the impact of captured assertions and assertion references, assertions that are consumed
2943 by an RP which is not part of the same Internet domain as the Verifier shall expire if they are not used within
2944 5 minutes of their creation.
2945 [KI-IAF: AL3_CM_VAS#110 a)]

³⁷ For example, implementation of SSO requires a separate assertion each time a new session is started with a participating RP.

- 2946 9.3.2.3.8 Assertions intended for use within a single Internet domain, including assertions contained in or
2947 referenced by cookies, however, may last as long as 12 hours without being used.
2948 [KI-IAF: AL3_CM_VAS#110 b)]
- 2949 9.3.2.3.9 If the underlying credential specifies that the subscriber name is a pseudonym, this information
2950 must be conveyed in the assertion.
2951 [KI-IAF: AL3_CM_VAS#040]
- 2952 9.3.2.3.10 Level 3 assertions shall be protected against manufacture/modification, capture, redirect and
2953 reuse. Assertion references shall be protected against manufacture, capture and reuse.
2954 [KI-IAF: AL3_CM_VAS#070 a, b)]
- 2955 9.3.2.3.11 Each assertion shall be targeted for a single RP
2956 [KI-IAF: AL3_CM_VAS#050]
- 2957 and the RP shall validate that it is the intended recipient of the incoming assertion.
2958 [KI-IAF: SAC do not apply to RPs, hence no mapping]
- 2959 9.3.2.3.12 Additionally, assertions, assertion references and any session cookies used by the Verifier or RP
2960 for authentication purposes, shall be transmitted to the Subscriber through a protected session which is linked
2961 to the primary authentication process in such a way that session hijacking attacks are resisted (see Section
2962 8.2.2 for methods which may be used to protect against session hijacking attacks).
2963 [KI-IAF: AL3_CM_VAS#070 c)]
- 2964 9.3.2.3.13 Assertions, assertion references and session cookies shall not be subsequently transmitted over an
2965 unprotected session or to an unauthenticated party while they remain valid.
2966 [KI-IAF: AL3_CM_VAS#070 c)]
- 2967 9.3.2.3.14 (To this end, any session cookies used for authentication purposes shall be flagged as secure, and
2968 redirects used to forward secondary authenticators from the Subscriber to the RP shall specify a secure
2969 protocol such as HTTPS.)
2970 [KI-IAF: AL3_CM_VAS#070 c)]
- 2971 9.3.2.3.15 To protect assertions against manufacture, modification, and disclosure, assertions which are sent
2972 from the Verifier to the RP, whether directly or through the Subscriber's device, shall either be sent via a
2973 mutually authenticated protected session between the Verifier and RP, or equivalently shall be signed by the
2974 Verifier and encrypted for the RP.
2975 [KI-IAF: AL3_CM_VAS#060 a & b)]
- 2976 9.3.2.3.16 All assertion protocols used at Level 2 and above require the use of Approved cryptographic
2977 techniques.
2978 [KI-IAF: AL3_CM_VAS#010]
- 2979 9.3.2.3.17 As such, the use of Kerberos keys derived from user-generated passwords is not permitted at
2980 Level 2 or above.
2981 [KI-IAF: AL3_CM_VAS#010 +NIST SP 800-63-2 Profiling]
- 2982 9.3.2.3.18 Assertions shall be protected against repudiation by the Verifier; all assertions used at Level 3
2983 shall be signed.
2984 [KI-IAF: AL3_CM_VAS#060]
- 2985 9.3.2.3.19 Level 3 assertions shall specify verified names and not pseudonyms.
2986 [KI-IAF: AL3_CM_VAS#040]

2987 9.3.2.3.20 Kerberos uses symmetric key mechanisms to protect key management and session data, and it
2988 does not protect against assertion repudiation. However, based on the high degree of vetting conducted on the
2989 Kerberos protocol and its wide deployment, Kerberos tickets are acceptable for use as assertions at Level 3 as
2990 long as:

- 2991 a) All Verifiers (Kerberos Authentication Servers and Ticket Granting Servers) are under the
2992 control of a single management authority that ensures the correct operation of the Kerberos protocol;
- 2993 b) The Subscriber is authenticated by the Verifier using a Level 3 token;
- 2994 c) All Level 3 requirements unrelated to non-repudiation are satisfied.

2995 [KI-IAF: AL3_CM_VAS#060 +NIST SP 800-63-2 Profiling]

2996 9.3.2.3.21 Also, at Level 3, single-domain assertions (e.g., Web browser cookies) shall expire if they are not
2997 used within 30 minutes.

2998 [KI-IAF: AL3_CM_VAS#110 b)]

2999 9.3.2.3.22 Cross-domain assertions shall expire if not used within 5 minutes.

3000 [KI-IAF: AL3_CM_VAS#110 a)]

3001 9.3.2.3.23 However, in order to deliver the effect of Single Sign On, the Verifier may re-authenticate the
3002 Subscriber prior to delivering assertions to new RPs, using a combination of long term and short term single-
3003 domain assertions, provided that the following assurances are met:

- 3004 a) The Subscriber has been successfully authenticated ~~to~~by the Verifier within the last 12 hours;
- 3005 b) The Subscriber can demonstrate that he or she was the party that was authenticated ~~by~~to the
3006 Verifier. This could be demonstrated, for example, by the presence of a cookie set by the
3007 Verifier in the Subscriber's browser;
- 3008 c) The Verifier can reliably determine whether the Subscriber has been in active communication
3009 with an RP since the last assertion was delivered by the Verifier. This means that the Verifier
3010 needs evidence that the Subscriber is actively using the services of the RP and has not been
3011 idle for more than 30 minutes. An authenticated assertion by the RP to this effect is considered
3012 sufficient evidence for this purpose.

3013 [KI-IAF: AL3_CM_VAS#120]

3014 9.3.2.4. Level 4

3015 9.3.2.4.0 All Level 1-3 requirements for the protection of assertion data remain in force at Level 4.

3016 [KI-IAF: Which are repeated as '4.1 to '4.23, so as to provide consistent mapping.]

3017 9.3.2.4.1 At Level 4, it must be impractical for an Attacker to manufacture an assertion or assertion
3018 reference that can be used to impersonate the Subscriber.

3019 [KI-IAF: AL4_CM_VAS#060 b, c)]

3020 9.3.2.4.2 If the direct model is used, the assertion which is used shall be signed by the Verifier or integrity-
3021 protected using a secret key shared by the Verifier and RP, and if the indirect model is used, the assertion
3022 reference which is used shall have a minimum of 64 bits of entropy.

3023 [KI-IAF: AL4_CM_VAS#060 b, c)]

- 3024 9.3.2.4.3 Bearer assertions shall be specific to a single transaction.³⁸
3025 [KI-IAF: AL4_CM_VAS#080]
- 3026 9.3.2.4.4 Also, if assertion references are used, they shall be freshly-generated whenever a new assertion is
3027 created by the Verifier. In other words, bearer assertions and assertion references are generated for one-time
3028 use.
3029 [KI-IAF: AL4_CM_VAS#090]
- 3030 9.3.2.4.5 Furthermore, in order to protect assertions against modification in the indirect model, all
3031 assertions sent from the Verifier to the RP shall either be signed by the Verifier, or transmitted from an
3032 authenticated Verifier via a protected session.
3033 [KI-IAF: AL4_CM_VAS#060 d)]
- 3034 9.3.2.4.6 In either case, a strong mechanism must be in place which allows the RP to establish a binding
3035 between the assertion reference and its corresponding assertion, based on integrity protected (or signed)
3036 communications with the authenticated Verifier.
3037 [KI-IAF: AL4_CM_VAS#100]
- 3038 9.3.2.4.7 To lessen the impact of captured assertions and assertion references, assertions that are consumed
3039 by an RP which is not part of the same Internet domain as the Verifier shall expire if they are not used within
3040 5 minutes of their creation.
3041 [KI-IAF: AL4_CM_VAS#110 a)]
- 3042 9.3.2.4.8 Assertions intended for use within a single Internet domain, including assertions contained in or
3043 referenced by cookies, however, may last as long as 12 hours without being used.
3044 [KI-IAF: AL4_CM_VAS#110 b)]
- 3045 9.3.2.4.9 If the underlying credential specifies that the subscriber name is a pseudonym, this information
3046 must be conveyed in the assertion.
3047 [KI-IAF: AL4_CM_VAS#040]
- 3048 9.3.2.4.10 Level 4 assertions shall be protected against manufacture/modification, capture, redirect and
3049 reuse. Assertion references shall be protected against manufacture, capture and reuse.
3050 [KI-IAF: AL4_CM_VAS#070 a, b)]
- 3051 9.3.2.4.11 Each assertion shall be targeted for a single RP
3052 [KI-IAF: AL4_CM_VAS#050]
- 3053 and the RP shall validate that it is the intended recipient of the incoming assertion.
3054 [KI-IAF: SAC do not apply to RPs, hence no mapping]
- 3055 9.3.2.4.12 Additionally, assertions, assertion references and any session cookies used by the Verifier or RP
3056 for authentication purposes, shall be transmitted to the Subscriber through a protected session which is linked
3057 to the primary authentication process in such a way that session hijacking attacks are resisted (see Section
3058 8.2.2 for methods which may be used to protect against session hijacking attacks).
3059 [KI-IAF: AL4_CM_VAS#070 c)]
- 3060 9.3.2.4.13 Assertions, assertion references and session cookies shall not be subsequently transmitted over an
3061 unprotected session or to an unauthenticated party while they remain valid.
3062 [KI-IAF: AL4_CM_VAS#070 c)]

³⁸ For example, implementation of SSO requires a separate assertion each time a new session is started with a participating RP.

- 3063 9.3.2.4.14 (To this end, any session cookies used for authentication purposes shall be flagged as secure, and
3064 redirects used to forward secondary authenticators from the Subscriber to the RP shall specify a secure
3065 protocol such as HTTPS.)
3066 [KI-IAF: AL4_CM_VAS#070 c)]
- 3067 9.3.2.4.15 To protect assertions against manufacture, modification, and disclosure, assertions which are sent
3068 from the Verifier to the RP, whether directly or through the Subscriber’s device, shall either be sent via a
3069 mutually authenticated protected session between the Verifier and RP, or equivalently shall be signed by the
3070 Verifier and encrypted for the RP.
3071 [KI-IAF: AL4_CM_VAS#060 b)]
- 3072 9.3.2.4.16 All assertion protocols used at Level 4 and above require the use of Approved cryptographic
3073 techniques.
3074 [KI-IAF: AL4_CM_VAS#010]
- 3075 9.3.2.4.17 As such, the use of Kerberos keys derived from user-generated passwords is not permitted at
3076 Level 4 or above.
3077 [KI-IAF: AL4_CM_VAS#010 +NIST SP 800-63-2 Profiling]
- 3078 9.3.2.4.18 Assertions shall be protected against repudiation by the Verifier; all assertions used at Level 4
3079 shall be signed.
3080 [KI-IAF: AL4_CM_VAS#060]
- 3081 9.3.2.4.19 Level 3 assertions shall specify verified names and not pseudonyms.
3082 [KI-IAF: AL4_CM_VAS#040]
- 3083 9.3.2.4.20 Kerberos uses symmetric key mechanisms to protect key management and session data, and it
3084 does not protect against assertion repudiation. However, based on the high degree of vetting conducted on the
3085 Kerberos protocol and its wide deployment, Kerberos tickets are acceptable for use as assertions at Level 4 as
3086 long as:
- 3087 a) All Verifiers (Kerberos Authentication Servers and Ticket Granting Servers) are under the
3088 control of a single management authority that ensures the correct operation of the Kerberos
3089 protocol;
 - 3090 b) The Subscriber is authenticated by the Verifier using a Level 4 token;
 - 3091 c) All Level 3 requirements unrelated to non-repudiation are satisfied.
- 3092 [KI-IAF: AL4_CM_VAS#060+NIST SP 800-63-2 Profiling]
- 3093 9.3.2.4.21 Also, at Level 4, single-domain assertions (e.g., Web browser cookies) shall expire if they are not
3094 used within 30 minutes.
3095 [KI-IAF: AL4_CM_VAS#110 b)]
- 3096 9.3.2.4.22 Cross-domain assertions shall expire if not used within 5 minutes.
3097 [KI-IAF: AL4_CM_VAS#110 a)]
- 3098 9.3.2.4.23 No stipulation
3099 [KI-IAF: SSO is specifically cited in SP 800-63-2 at AL3 and AL4 requires only the same protections of assertion data as were
3100 applied at AL1 – AL3, but does not relate to how such assertions may be used, hence omitted in this mapping at AL4.]

3101 9.3.2.4.24 At Level 4, bearer assertions (including cookies) shall not be used to establish the identity of the
3102 Claimant to the RP.
3103 [KI-IAF: AL4_CM_VAS#020]

3104 9.3.2.4.25 Assertions made by the Verifier may however be used to bind keys or other attributes to an
3105 identity. Holder-of-key assertions may be used, provided that all three requirements below are met:

3106 a) The Claimant **must be** authenticated ~~to~~ **by** the Verifier using a Level 4 token (as described in
3107 Section 6) in a Level 4 authentication protocol (as described in Section 8).

3108 b) The Verifier generates a holder-of-key assertion that references a key that is part of the Level
3109 4 token (used to authenticate to the Verifier) or linked to it through a chain of trust, and;

3110 c) The RP verifies that the Subscriber possesses the key that is referenced in the holder-of-key
3111 assertion using a Level 4 protocol (where the RP plays the role attributed to the Verifier by
3112 Section 8).

3113 [KI-IAF: SAC do not apply to RPs, hence no mapping]

3114 9.3.2.4.26 The RP should maintain records of the assertions it receives, so that if a suspicious transaction
3115 occurs at the RP, the key asserted by the Verifier may be compared to the value registered with the CSP.

3116 [KI-IAF: SAC do not apply to RPs, hence no mapping]

3117 This record keeping allows the RP to detect any attempt by the Verifier to impersonate the Subscriber using
3118 fraudulent assertions and may also be useful for preventing the Subscriber from repudiating various aspects
3119 of the authentication process.

3120

3121 **10. References**

3122 This section lists references that are current versions at the time of publication. Subsequent versions of NIST
3123 publications (i.e., Federal Information Processing Standards and Special Publications) are also acceptable.

3124 **10.1. General References**

- 3125 [DOJ 2000] *Guide to Federal Agencies on Implementing Electronic Processes* (November 2000),
3126 available at: <http://www.usdoj.gov/criminal/cybercrime/ecommerce.html>
3127
- 3128 [GSA ESIG] *Use of Electronic Signatures in Federal Organization Transactions* (2011), available at:
3129 <http://www.gsa.gov/>
3130
- 3131 [FISMA] *Federal Information Security Management Act*, available at:
3132 <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>
3133
- 3134 [OMB M-04-04] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal agencies*,
3135 December 16, 2003, available at:
3136 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
3137
- 3138 [OMB M-03-22] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions*
3139 *of the E-Government Act of 2002*, September 26, 2003 available at:
3140 <http://www.whitehouse.gov/omb/memoranda/m03-22.html>.
- 3141 [KERB] Neuman, C., and T. Ts'o, *Kerberos: An Authentication Service for Computer Networks*,
3142 IEEE Communications, vol. 32, no.9, 1994.
- 3143 [RFC 4120] IETF, RFC 4120, *The Kerberos Network Authentication Service (V5)*, July 2005,
3144 available at <http://www.ietf.org/rfc/rfc4120.txt>
- 3145 [RFC 1939] IETF, RFC 1939, *Post Office Protocol*, Version 3, May 1996, available at:
3146 <http://www.ietf.org/rfc/rfc1939.txt>
- 3147 [RFC 2246] IETF, RFC 2246, *The TLS Protocol*, Version 1.0. January 1999, available at:
3148 <http://www.ietf.org/rfc/rfc2246.txt>
- 3149 [RFC 5280] IETF, RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*,
3150 available at: <http://www.ietf.org/rfc/rfc5280.txt>
- 3151 [RFC 3546] IETF, RFC 3546, *Transport Layer Security (TLS) Extensions*, June 2003, available at:
3152 <http://www.ietf.org/rfc/rfc3546.txt>
- 3153 [RFC 5246] IETF, RFC 5246, *The Transport Layer Security (TLS) Protocol*, Version 1.2, August
3154 2008, available at <http://tools.ietf.org/html/rfc5246>
- 3155 [RFC 1760] IETF, RFC 1760, *The S/KEY One-Time Password System*, February 1995, available at:
3156 <http://www.ietf.org/rfc/rfc1760.txt>
- 3157 [ICAM] National Security Systems and Identity, Credential and Access Management Sub-
3158 Committee Focus Group, Federal CIO Council, *ICAM Lexicon*, Version 0.5, March 2011.
- 3159 [ISPKI] ITU-T Recommendation X.509 | ISO / IEC 9594-8: “Information Technology - Open
3160 Systems Interconnection - The Directory: Public-Key and Attribute Certificate
3161 Frameworks.”

3162 [SAML] OASIS, SAML, “Security Assertion Markup Language 2.0,” v2.0, March 2005, available
3163 at
3164 <http://www.oasis-open.org/standards#samlv2.0>

3165

3166 **10.2. NIST Special Publications**

3167 NIST 800 Series Special Publications are available at: <http://csrc.nist.gov/publications/nistpubs/index.html>.
3168 The following publications may be of particular interest to those implementing systems of applications
3169 requiring e-authentication.
3170

3171 [SP 800-30] NIST Special Publication 800-30, *Risk Management Guide for Information Technology*
3172 *Systems*, July 2002.

3173 [SP 800-32] NIST Special Publication, 800-32, *Introduction to Public Key Technology and the*
3174 *Federal PKI Infrastructure*, February 2001.

3175 [SP 800-33] NIST Special Publication 800-33, *Underlying Technical Models for Information*
3176 *Technology Security*, December 2001.

3177 [SP 800-37] NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management*
3178 *Framework to Federal Information Systems*, February 2010.

3179 [SP 800-40] NIST Special Publication 800-40, Version 2.0, *Creating a Patch and Vulnerability*
3180 *Management Program*, November 2005.

3181 [SP 800-41] NIST Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall*
3182 *Policy*, September 2009.

3183 [SP 800-43] NIST Special Publication 800-43, *Guide to Securing Windows 2000 Professional*,
3184 November 2002.

3185 [SP 800-44] NIST Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*,
3186 September 2007.

3187 [SP 800-47] NIST Special Publication 800-47, *Security Guide for Interconnecting Information*
3188 *Technology Systems*, September 2002.

3189 [SP 800-52] NIST Special Publication 800-52, *Guidelines for the Selection and Use of Transport*
3190 *Layer Security Implementations*, June 2005.

3191 [SP 800-53] NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for*
3192 *Federal Information Systems and Organizations*, August 2009 and Errata as of May
3193 2010.

3194 [SP 800-53A] NIST Special Publication 800-53A, Revision 1, *Guide for Assessing the Security*
3195 *Controls in Federal Information Systems and Organizations, Building Effective Security*
3196 *Assessment Plans*, June 2010.

3197 [SP 800-57] NIST Special Publication 800-57, Revision 2, *Recommendation for Key Management –*
3198 *Part 1: General*, March 2007.

3199 [SP 800-94] NIST Special Publication, 800-94, *Guide to Intrusion Detection and Prevention Systems*
3200 *(IDPS)*, February 2007.

3201 [SP 800-115] NIST Special Publication 800-115, *Technical Guide to Information Security Testing and*
3202 *Assessment*, September 2008.

3203

3204 **10.3. Federal Information Processing Standards**

3205 FIPS can be found at: <http://csrc.nist.gov/publications/fips/>

3206

3207 [FIPS 140-2] Federal Information Processing Standard Publication 140-2, *Security Requirements for*
3208 *Cryptographic Modules*, NIST, May 25, 2001.

3209 [FIPS 180-2] Federal Information Processing Standard Publication 180-2, *Secure Hash Standard*
3210 *(SHS)*, NIST, August 2002.

3211 [FIPS186-2] Federal Information Processing Standard Publication 186-2, *Digital Signature Standard*
3212 *(DSS)*, NIST, June 2000.

3213 [FIPS 197] Federal Information Processing Standard Publication 197, *Advanced Encryption Standard*
3214 *(AES)*, NIST, November 2001.

3215 [FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*
3216 (February 2004), available at:

3217 <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

3218

3219 [FIPS 201] *Personal Identity Verification (PIV) of Federal Employees and Contractors* (March
3220 2006), available at:

3221 <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

3222

3223 **10.4. Certificate Policies**

3224 These certificate policies can be found at: <http://www.cio.gov/fpkipa/>

3225 [FBCA1] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, version
3226 2.1 January 12, 2006. Available at:

3227 http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

3228 [FBCA2] *Citizen & Commerce Certificate Policy*, Version 1.0 December 3, 2002. Available at:

3229 http://www.cio.gov/fpkipa/documents/citizen_commerce_cp1.pdf

3230 [FBCA3] *X.509 Certificate Policy for the Common Policy Framework*, Version 2.4 February 15,
3231 2006. Available at: <http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf>

3232 **Appendix A: Estimating Entropy and Strength**

3233 **Password Entropy**

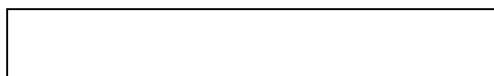
3234

3235 Passwords represent a very popular implementation of memorized secret tokens. In this case impersonation
3236 of an identity requires only that the impersonator obtain the password. Moreover, the ability of humans to
3237 remember long, arbitrary passwords is limited, so passwords are often vulnerable to a variety of attacks
3238 including guessing, use of dictionaries of common passwords, and brute force attacks of all possible
3239 password combinations. There are a wide variety of password authentication protocols that differ

3240 significantly in their vulnerabilities, and many password mechanisms are vulnerable to passive and active
3241 network attacks. While some cryptographic password protocols resist nearly all direct network attacks, these
3242 techniques are not at present widely used and all password authentication mechanisms are vulnerable to
3243 keyboard loggers and observation of the password when it is entered. Experience also shows that users are
3244 vulnerable to “social engineering” attacks where they are persuaded to reveal their passwords to unknown
3245 parties, who are basically “confidence men.”

3246 Claude Shannon coined the use of the term “entropy³⁹” in information theory. The concept has many
3247 applications to information theory and communications and Shannon also applied it to express the amount of
3248 actual information in English text. Shannon says, “The entropy is a statistical parameter which measures in a
3249 certain sense, how much information is produced on the average for each letter of a text in the language. If
3250 the language is translated into binary digits (0 or 1) in the most efficient way, the entropy H is the average
3251 number of binary digits required per letter of the original language.”⁴⁰

3252 Entropy in this sense is at most only loosely related to the use of the term in thermodynamics. A
3253 mathematical definition of entropy in terms of the probability distribution function is:



3254 where $P(X=x)$ is the probability that the variable X has the value x .

3255 Shannon was interested in strings of ordinary English text and how many bits it would take to code them in
3256 the most efficient way possible. Since Shannon coined the term, “entropy” has been used in cryptography as
3257 a measure of the difficulty in guessing or determining a password or a key. Clearly the strongest key or
3258 password of a particular size is a truly random selection, and clearly, on average such a selection cannot be
3259 compressed. However it is far from clear that compression is the best measure for the strength of keys and
3260 passwords, and cryptographers have derived a number of alternative forms or definitions of entropy,
3261 including “guessing entropy” and “min-entropy.” As applied to a distribution of passwords the guessing
3262 entropy is, roughly speaking, an estimate of the average amount of work required to guess the password of a
3263 selected user, and the min-entropy is a measure of the difficulty of guessing the easiest single password to
3264 guess in the population.

3265 If we had a good knowledge of the frequency distribution of passwords chosen under a particular set of rules,
3266 then it would be straightforward to determine either the guessing entropy or the min-entropy of any
3267 password. An Attacker who knew the password distribution would find the password of a chosen user by first
3268 trying the most probable password for that chosen username, then the second most probable password for
3269 that username and so on in decreasing order of probability until the Attacker found the password that worked
3270 with the chosen username. The average for all passwords would be the guessing entropy. The Attacker who
3271 is content to find the password of any user would follow a somewhat different strategy, he would try the most
3272 probable password with every username, then the second most probable password with every username, until
3273 he found the first “hit.” This corresponds to the min-entropy.

3274 Unfortunately, we do not have much data on the passwords users choose under particular rules, and much of
3275 what we do know is found empirically by “cracking” passwords, that is by system administrators applying
3276 massive dictionary attacks to the files of hashed passwords (in most systems no plaintext copy of the
3277 password is kept) on their systems. NIST would like to obtain more data on the passwords users actually

³⁹ C. E. Shannon, “A mathematical Theory of Communication,” *Bell System Technical Journal*, v. 27, pp. 379-423, 623-656, July, October 1948, see <http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html>

⁴⁰ C. E. Shannon, “Prediction and Entropy of Printed English,” *Bell System Technical Journal*, v.30, n. 1, 1951, pp. 50-64.

3278 choose, but, where they have the data, system administrators are understandably reluctant to reveal password
3279 data to others. Empirical and anecdotal data suggest that many users choose very easily guessed passwords,
3280 where the system will allow them to do so.

3281 **A.1 Randomly Selected Passwords**

3282
3283 As we use the term here, “entropy” denotes the uncertainty in the value of a password. Entropy of passwords
3284 is conventionally expressed in bits. If a password of k bits is chosen at random there are 2^k possible values
3285 and the password is said to have k bits of entropy. If a password of length l characters is chosen at random
3286 from an alphabet of b characters (for example the 94 printable ISO characters on a typical keyboard) then the
3287 entropy of the password is b^l (for example if a password composed of 8 characters from the alphabet of 94
3288 printable ISO characters the entropy is $94^8 \approx 6.09 \times 10^{15}$ – this is about 2^{52} , so such a password is said to have
3289 about 52 bits of entropy). For randomly chosen passwords, guessing entropy, min-entropy, and Shannon
3290 entropy are all the same value. The general formula for entropy, H is given by:

$$3291 \quad H = \log_2 (b^l)$$

3292

3293 Table A.1 gives the entropy versus length for a randomly generated password chosen from the standard 94
3294 keyboard characters (not including the space). Calculation of randomly selected passwords from other
3295 alphabets is straightforward.

3296

3297 **A.2 User Selected Passwords**

3298
3299 It is much more difficult to estimate the entropy in passwords that users choose for themselves, because they
3300 are not chosen at random and they will not have a uniform random distribution. Passwords chosen by users
3301 probably roughly reflect the patterns and character frequency distributions of ordinary English text, and are
3302 chosen by users so that they can remember them. Experience teaches us that many users, left to choose their
3303 own passwords will choose passwords that are easily guessed and even fairly short dictionaries of a few
3304 thousand commonly chosen passwords, when they are compared to actual user chosen passwords, succeed in
3305 “cracking” a large share of those passwords.

3306 **A.2.1 Guessing Entropy Estimate**

3307

3308 Guessing entropy is arguably the most critical measure of the strength of a password system, since it largely
3309 determines the resistance to targeted, online password guessing attacks.

3310 In these guidelines, we have chosen to use Shannon’s estimate of the entropy in ordinary English text as the
3311 starting point to estimate the entropy of user-selected passwords. It is a big assumption that passwords are
3312 quite similar to other English text, and it would be better if we had a large body of actual user selected
3313 passwords, selected under different composition rules, to work from, but we have no such resource, and it is
3314 at least plausible to use Shannon’s work for a “ballpark” estimate. Readers are cautioned against interpreting
3315 the following rules as anything more than a very rough rule of thumb method to be used for the purposes of
3316 e-authentication.

3317 Shannon conducted experiments where he gave people strings of English text and asked them to guess the
3318 next character in the string. From this he estimated the entropy of each successive character. He used a 27-
3319 character alphabet, the ordinary English lower case letters plus the space.

3320 In the following discussion we assume that passwords are user selected from the normal keyboard alphabet
3321 of 94 printable characters, and are at least 6-characters long. Since Shannon used a 27 character alphabet it
3322 may seem that the entropy of user selected passwords would be much larger, however the assumption here is
3323 that users will choose passwords that are almost entirely lower case letters, unless forced to do otherwise, and
3324 that rules that force them to include capital letters or non-alphabetic characters will generally be satisfied in
3325 the simplest and most predictable manner, often by putting a capital letter at the start (as we do in ordinary
3326 English) and punctuation or special characters at the end, or by some simple substitution, such as \$ for the
3327 letter “s.” Moreover rules that force passwords to appear to be highly random will be counterproductive
3328 because they will make the passwords hard to remember. Users will then write the passwords down and keep
3329 them in a convenient (that is insecure) place, such as pasted on their monitor. Therefore it is reasonable to
3330 start from estimates of the entropy of simple English text, assuming only a 27-symbol alphabet.

3331 Shannon observed that, although there is a non-uniform probability distribution of letters, it is comparatively
3332 hard to predict the first letter of an English text string, but, given the first letter, it is much easier to guess the
3333 second and given the first two the third is easier still, and so on. He estimated the entropy of the first symbol
3334 at 4.6 to 4.7 bits, declining to on the order of about 1.5 bits after 8 characters. Very long English strings (for
3335 example the collected works of Shakespeare) have been estimated to have as little as .4 bits of entropy per
3336 character.⁴¹ Similarly, in a string of words, it is harder to predict the first letter of a word than the following
3337 letters, and the first letter carries about 6 times more information than the fifth or later letters⁴².

3338 An Attacker attempting to find a password will try the most likely chosen passwords first. Very extensive
3339 dictionaries of passwords have been created for this purpose. Because users often choose common words or
3340 very simple passwords systems commonly impose rules on password selection in an attempt to prevent the
3341 choice of “bad” passwords and improve the resistance of user chosen passwords to such dictionary or rule
3342 driven password guessing attacks. For the purposes of these guidelines, we break those rules into two
3343 categories:

- 3344 1. Dictionary tests that test prospective passwords against an “extensive dictionary test” of common
3345 words and commonly used passwords, then disallow passwords found in the dictionary. We do not
3346 precisely define a dictionary test, since it must be tailored to the password length and rules, but it
3347 should prevent selection of passwords that are simple transformations of any one word found in an
3348 unabridged English [KI-IAF:and/ or any other appropriate natural-language dictionary, according to
3349 the scope of use] dictionary, and should include at least 50,000 words. There is no intention to prevent
3350 selection of long passwords (16 characters or more based on phrases) and no need to impose a
3351 dictionary test on such long passwords of 16 characters or more.
- 3352 2. Composition rules that typically require users to select passwords that include lower case letters,
3353 upper case letters, and non-alphabetic symbols (e.g.:: “~!@#\$\$%^&*()_-
3354 +={ }[]\|:;’<,.>./1234567890”).

3355
3356 Either dictionary tests or composition rules eliminate some passwords and reduce the space that an adversary
3357 must test to find a password in a guessing or exhaustion attack. However they can eliminate many obvious
3358 choices and therefore we believe that they generally improve the “practical entropy” of passwords, although

⁴¹ Thomas Schurmann and Peter Grassberger, “Entropy estimation of symbol sequences,” <http://arxiv.org/ftp/cond-mat/papers/0203/0203436.pdf>

⁴² *ibid.*

3359 they reduce the work required for a truly exhaustive attack. The dictionary check requires a dictionary of at
3360 least 50,000 legal passwords chosen to exclude commonly selected passwords. Upper case letters in
3361 candidate passwords should be converted to lower case before comparison.

3362 Table A.1 provides a rough estimate of the average entropy of user chosen passwords as a function of
3363 password length. Estimates are given for user selected passwords drawn from the normal keyboard alphabet
3364 that are not subject to further rules, passwords subject to a dictionary check to prevent the use of common
3365 words or commonly chosen passwords and passwords subject to both composition rules and a dictionary test.
3366 In addition an estimate is provided for passwords or PINs with a ten-digit alphabet. The table also shows the
3367 calculated entropy of randomly selected passwords and PINs. The values of Table A.1 should not be taken as
3368 accurate estimates of absolute entropy, but they do provide a rough relative estimate of the likely entropy of
3369 user chosen passwords, and some basis for setting a standard for password strength.

3370 The logic of the Table A.1 is as follows for user-selected passwords drawn from the full keyboard alphabet:

- 3371 a) The entropy of the first character is taken to be 4 bits;
- 3372 b) The entropy of the next 7 characters are 2 bits per character; this is roughly consistent with
3373 Shannon’s estimate that “when statistical effects extending over not more than 8 letters are
3374 considered the entropy is roughly 2.3 bits per character;”
- 3375 c) For the 9th through the 20th character the entropy is taken to be 1.5 bits per character;
- 3376 d) For characters 21 and above the entropy is taken to be 1 bit per character;
- 3377 e) A “bonus” of 6 bits of entropy is assigned for a composition rule that requires both upper case
3378 and non-alphabetic characters. This forces the use of these characters, but in many cases these
3379 characters will occur only at the beginning or the end of the password, and it reduces the total
3380 search space somewhat, so the benefit is probably modest and nearly independent of the
3381 length of the password;
- 3382 f) A bonus of up to 6 bits of entropy is added for an extensive dictionary check. If the Attacker
3383 knows the dictionary, he can avoid testing those passwords, and will in any event, be able to
3384 guess much of the dictionary, which will, however, be the most likely selected passwords in
3385 the absence of a dictionary rule. The assumption is that most of the guessing entropy benefits
3386 for a dictionary test accrue to relatively short passwords, because any long password that can
3387 be remembered must necessarily be a “pass-phrase” composed of dictionary words, so the
3388 bonus declines to zero at 20 characters.

3389 For user selected PINs the assumption of Table A.1 is that such pins are subjected at least to a rule that
3390 prevents selection of all the same digit, or runs of digits (e.g., “1234” or “76543”). This column of Table A.1
3391 is at best a very crude estimate, and experience with password crackers suggests, for example, that users will
3392 often preferentially select simple number patterns and recent dates, for example their year of birth.

3393 **A.2.2 Min-Entropy Estimates**

3394 Experience suggests that a significant share of users will choose passwords that are very easily guessed
3395 (“password” may be the most commonly selected password, where it is allowed). Suppose, for example, that
3396 one user in 1,000 chooses one of the 2 most common passwords, in a system that allows a user 3 tries before
3397 locking a password. An Attacker with a list of user names, who knows the two most commonly chosen
3398 passwords can use an automated attack to try those 2 passwords with each user name, and can expect to find
3399 at least one password about half the time by trying 700 usernames with those two passwords. Clearly this is a
3400
3401

3402 practical attack if the only goal is to get access to the system, rather than to impersonate a single selected
3403 user. This is usually too dangerous a possibility to ignore.

3404 We know of no accurate general way to estimate the actual min-entropy of user chosen passwords, without
3405 examining in detail the passwords that users actually select under the rules of the password system, however
3406 it is reasonable to argue that testing user chosen passwords against a sizable dictionary of otherwise
3407 commonly chosen legal passwords, and disallowing matches, will raise the min-entropy of a password. A
3408 dictionary test is specified here that is intended to ensure at least 10 bits of min-entropy. That test is:

- 3409 a) Upper case letters in passwords are converted to entirely lower case and compared to a
3410 dictionary of at least 50,000 commonly selected otherwise legal passwords and rejected if they
3411 match any dictionary entry, and
- 3412 b) Passwords that are detectable permutations of the username are not allowed.

3413 This is estimated to ensure at least 10 bits of min-entropy. Other means may be substituted to ensure at least
3414 10 bits of min-entropy. User chosen passwords of at least 15 characters are assumed to have at least 10 bits of
3415 min-entropy. For example a user might be given a short randomly chosen string (two randomly chosen
3416 characters from a 94-bit alphabet have about 13 bits of entropy). A password, for example, might combine
3417 short system selected random elements, to ensure 10 bits of min-entropy, with a longer user-chosen
3418 password.

3419

3420 **A.3 Other Types of Passwords**

3421 Some password systems require a user to memorize a number of images, such as faces. Users are then
3422 typically presented with successive fields of several images (typically 9 at a time), each of which contains
3423 one of the memorized images. Each selection represents approximately 3.17 bits of entropy. If such a system
3424 used five rounds of memorized images, then the entropy of system would be approximately 16 bits. Since
3425 this is randomly selected password the guessing entropy and min-entropy are both the same value.
3426

3427 It is possible to combine randomly chosen and user chosen elements into a single composite password. For
3428 example a user might be given a short randomly selected value to ensure min-entropy to use in combination
3429 with a user chosen password string. The random component might be images or a character string.

Table A.1 – Estimated Password Guessing Entropy in bits vs. Password Length

Length Char.	User Chosen			Randomly Chosen		
	94 Character Alphabet			10 char. alphabet	94 char alphabet	
	No Checks	Dictionary Rule	Dict. & Composition Rule			
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

3430 Figure A.1 - Estimated User Selected Password Entropy vs. Length
 3431

3432

3433 **Appendix B: Mapping of Federal PKI Certificate Policies to E-authentication** 3434 **Assurance Levels**

3435

3436 Agencies are, in general, issuing certificates under the policies specified in the Common Policy Framework
3437 [FBCA3] to satisfy FIPS 201. Organizations outside the US Government have begun issuing credentials
3438 under a parallel set of policies and requirements known collectively as PIV Interoperability specifications
3439 (PIV-I). Agencies that were early adopters of PKI technology, and organizations outside the Federal
3440 government, issue PKI certificates under organization specific policies instead of the Common Policy
3441 Framework. The primary mechanism for evaluating the assurance provided by public key certificates issued
3442 under organization specific policies is the policy mapping of the Federal Policy Authority to the Federal
3443 Bridge CA policies. These policies include the Rudimentary, Basic, Medium, Medium-HW, and High
3444 assurance policies specified in [FBCA1] and the Citizen and Commerce class policy specified in [FBCA2].

3445 These policies incorporate all aspects of the credential lifecycle, often in greater detail than specified here.
3446 These policies also include security controls (e.g., multi-party control and system auditing for CSPs) that are
3447 outside the scope of this document. However, the FPKI policies are based on work that largely predates this
3448 specification, and the security requirements are not always strictly aligned with those specified here. As a
3449 result, this appendix provides an overall mapping between FPKI certificate policies and the e-authentication
3450 Levels instead of a strict evaluation of compliance. There are known discrepancies, such as FIPS 201's
3451 allowance for pseudonyms on credentials issued to personnel in dangerous jobs, or the ability to issue PIV
3452 credentials based on a single federal government issued identity credential. While these discrepancies are
3453 recognized, the overall level of assurance provided by these policies is deemed to meet the requirements
3454 based on the additional controls.

3455 The table below summarizes how certificates issued under the Common Policy Framework correspond to the
3456 e-authentication assurance levels. Note that the Common Device policy is not listed; this policy supports
3457 authentication of a system rather than a person. In addition, table B.1 ([following page](#)) summarizes how
3458 organization specific certificate policies correspond to e-authentication assurance levels. At Level 2 agencies
3459 may use certificates issued under policies that have not been mapped by the Federal policy authority, but are
3460 determined to meet the Level 2 identify proofing, token and status reporting requirements. (For this
3461 evaluation, a strict compliance mapping should be used, rather than the rough mapping used for the FPKI
3462 policies.) For Levels 3 and 4, agencies shall depend upon the mappings provided by the Federal PKI.

3463 The Federal PKI has also added two policies, Medium Commercial Best Practices (Medium-CBP) and
3464 Medium Hardware Commercial Best Practices (MediumHW-CBP) to support recognition of non-Federal
3465 PKIs. In terms of e-authentication levels, the Medium CBP and MediumHW-CBP are equivalent to Medium
3466 and Medium-HW, respectively.

3467

3468
 3469
 3470

Table B.1 – Certificate Policies and the E-authentication Assurance Levels

Certificate Policy	Selected Policy Components			Overall Equivalence
	Identity Proofing	Token	Token and Credential Management ⁴³	
Common-Auth PIVI-Auth SHA1-Auth ⁴⁴	Meets Level 4	Meets Level 4	Meets Level 4	Meets Level 4
Common-SW	Meets Level 4	Meets Level 3	Meets Level 4	Meets Level 3
Common-HW PIVI-HW SHA1-HW ⁴⁴	Meets Level 4	Meets Level 4	Meets Level 4	Meets Level 4
Common-High	Meets Level 4	Meets Level 4	Meets Level 4	Meets Level 4
FBCA Basic ⁴⁵	Meets Level 3	Meets Level 3	Meets Level 3	Meets Level 3
FBCA Medium ⁴⁵	Meets Level 4	Meets Level 3	Meets Level 4	Meets Level 3
FBCA Medium-HW ⁴⁵	Meets Level 4	Meets Level 4	Meets Level 4	Meets Level 4
FBCA High ⁴⁵	Meets Level 4	Meets Level 4	Meets Level 4	Meets Level 4
Common-cardAuth PIVI-cardAuth SHA1-cardAuth ⁴⁴	Meets Level 4	Meets Level 2	Meets Level 4	Meets Level 2

3471

⁴³ The key component in token and credential management is the credential status mechanism.

⁴⁴ The SHA1 policies have been deprecated and will not be acceptable after December 31, 2013.

⁴⁵ These policies are not asserted in the user certificates, but equivalence is established through policy mapping at the Federal Bridge CA.