Federal Identity, Credential, and Access Management Sub Committee

Security Controls Mapping of Special Publication 800-53 Revision 5, Identification and Authentication (IA), against Special Publication 800-63

Version 1.0

April 24, 2024

Revision History

Document Version	Document Date	Revision Details
1.0	04//24/2024	Initial Mapping of IA Controls

TABLE OF CONTENTS

Introduction

This document provides guidance for organizations who need to comply with the requirements of NIST SP 800-53 rev. 5 and NIST SP 800-63.

NIST SP 800-53 rev. 5 provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. The use of these controls is mandatory for federal information systems in accordance with Office of Management and Budget (OMB) Circular A-130 [OMB A-130] and the provisions of the Federal Information Security Modernization Act (FISMA), which requires the implementation of minimum controls to protect federal information and information systems.

NIST SP 800-63 guidelines lay out a model for federal programs and other organizations to assess and manage risks associated with digital identity systems, including the processes, policies, data, people, and technologies that support digital identity management. The model is supported by a series of processes: identity proofing, authentication, and federation. The identity proofing process establishes that a subject is a specific physical person. The digital authentication process determines the validity of one or more authenticators to claim a digital identity. It establishes confidence that a subject attempting to access a digital service: (1) is in control of the technologies being used for authentication and (2) is the same subject that previously accessed the service. Finally, the federation process allows shared identity information to support system authentication.

Additionally, NIST SP 800-63 provides instruction for credential service providers (CSPs), verifiers, and relying parties (RPs), and it describes the risk management processes that organizations should follow for implementing

digital identity services and that supplement the *NIST Risk Management Framework* and its special component publications.

NIST SP 800-63 guidelines focus on organizational services interacting with external users, such as citizens accessing public benefits or private sector partners accessing collaboration spaces. However, it also applies to federal systems accessed by employees and contractors.

A supplement to 800-63 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63Bsup1.pdf) was released as this mapping document was being finalized. The requirements of the supplement were not included in this document due to time constraints. Those updates may be reflected in a future version of this document.

Applicability and Use

This document contains two different mappings between 800-53 rev. 5 and 800-63. The first is an informational policy mapping. The mapping gives organizations a *general* indication of security and privacy control coverage concerning NIST SP 800-63 guidance. Accordingly, the mapping will help organizations better comply with certain NIST SP 800-53 rev. 5 controls by meeting NIST SP 800-63 digital identity assurance level guidance.
For each 800-53 rev. 5 control in scope, 800-63 sections with relevant background or discussion are identified. This enables readers to obtain context and understanding of the concepts in 800-63 that are relevant to the topic covered in the policy.

The second mapping is a policy crosswalk. The policy crosswalk identifies mappings between specific requirements in each document. This mapping provides specific information about equivalent controls in each respective document. Readers will be able to determine which specific requirements in 800-63 are relevant to a given control in 800-53 rev. 5, to assist in complying with both sets of requirements.

Informational Policy Mapping

Control	NIST SP 800-53 R5 Control	NIST SP 800-63 (Draft Version 4) Guidance
IA-1	a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]: 1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among	• 800-63-4 Sections 2.1, 4.1, 5.5 • 800-83C-4 Sections 5, 5.1 and subsections, 5.2 and subsections

Control	NIST SP 800-53 R5 Control	NIST SP 800-63 (Draft Version 4) Guidance
	organizational entities, and compliance; and	
	(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	• 800-63-4 Sections 2.3.1, 5, 5.1.2, 5.2.2.2 • 800-63A-4 Sections 4.3.3.2, 4.3.4.4, 5.1.2.1, 5.1.3, 5.1.5, 5.1.8, 5.1.10, 7, 8.3, 8.6, 9 • 800-63B-4 Sections 4, 4.1.2, 4.1.4, 4.1.5, 4.2.2, 4.2.4, 4.2.5, 4.3.2, 4.3.4, 4.3.5, 4.4, 5.1.1.2, 5.1.2.1, 5.1.3.2, 5.1.4.1, 5.1.5.1, 5.1.7.1, 5.1.9.1, 5.2.3, 5.2.4, 5.2.5, 5.2.7, 5.2.12, 6.1.2.3, 6.4, 7.1, 9.3, 9.4, 10, 10.4, 11 • 800-63C-4 Sections 4, 4.1, 4.2, 4.3, 5.2.2, 7.1, 9.1, 10, 11, 12.2, 12.3
	2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;	• 800-63-4 Section 5 and subsections • 800-63A-4 Sections 5.1.1, 5.1.1.1, 5.1.10, 10.3 fourth Description
IA-1	b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures;	No direct mapping. However, see 800-63A-4 Sections 5.1.5, 8.6, 800-63B-4 4.4, 9.4, 800-83C-4 5.5, 9.4 for officials to be consulted
IA-1	c. Review and update the current identification and authentication: 1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and 2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].	No direct mapping. However, see 800-63-4 Sections 5.3.2, 800-63A-4 5.1.1, 5.1.2.1, 5.1.3, 5.1.5, 800-63B-4 6.1.4
IA-2	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	• 800-63-4 Section 2.1, 4 and subsections • 800-63A-4 Section 4 and subsections, Section 5 and subsections. However, best to read 800-63A-4 in full • 800-63B-4 Sections 4 and subsections and 5 and subsections. However, it is best to read 800-63B-4 in full • For CSPs that operate identity proofing and enrollment services, see also 800-63A-4 Section 5 and subsections; Section 6.1 • 800-63B-4 Sections 4 and subsections; 6.1 and subsections; 6.1.2 and subsections; 6.1.3
IA-2(1)	Implement multi-factor authentication for access to privileged accounts.	• 800-63B-4 Sections 4.1, 4.1.1; 4.2, 4.2.1; 4.3, 4.3.1; 4.4, 4.4.1; 5.1.1; 5.1.3.4; 5.1.5 and subsections; 5.1.8 and subsections; 5.1.9 and subsections; 5.2.3; 10.2.5, 10.2.8, 10.2.9, 10.3
IA-2(2)	Implement multi-factor authentication for access to non-privileged accounts.	• 800-63B-4 Sections 4.1, 4.1.1; 4.2, 4.2.1; 4.3, 4.3.1; 4.4, 4.4.1; 5.1.1; 5.1.3.4; 5.1.5 and subsections; 5.1.8 and

Control	NIST SP 800-53 R5 Control	NIST SP 800-63 (Draft Version 4) Guidance
		subsections; 5.1.9 and subsections; 5.2.3; 10.2.5, 10.2.8, 10.2.9, 10.3
IA-2(5)	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.	• 800-63B-4 Section 4
IA-2(6)	Implement multi-factor authentication for [*Selection (one or more): local; network; remote*] access to [*Selection (one or more): privileged accounts; non-privileged accounts*] such that:	• 800-63B-4 Sections 4.1, 4.1.1; 4.2, 4.2.1; 4.3, 4.3.1; 4.4, 4.4.1; 5.1.1; 5.1.3.4; 5.1.5 and subsections; 5.1.8 and subsections; 5.1.9 and subsections; 5.2.3; 10.2.5, 10.2.8, 10.2.9, 10.3
	(a) One of the factors is provided by a device separate from the system gaining access; and	• 800-63B-4 Sections 4.2, 4.2.1, 4.3, 4.3.1, 5.1.3.4, 5.1.5, 5.1.8, 5.1.9
	(b) The device meets [*Assignment: organization-defined strength of mechanism requirements*].	• 800-63B-4 Section 4 and subsections, 4.5
IA-2(8)	Implement replay-resistant authentication mechanisms for access to [*Selection (one or more): privileged accounts; non-privileged accounts*].	• 800-63B-4 Sections 4.2.2, 4.3.2, Table 1, 5.1.3.2, 5.1.4.2, 5.1.5.2, 5.2.5, 5.2.8, Table 4
IA-2(10)	Provide a single sign-on capability for [*Assignment: organization-defined system accounts and services*].	• 800-63C-4
IA-2(12)	Accept and electronically verify Personal Identity Verification-compliant credentials.	No direct mapping. However, see 800-63B-4 Section 5.1.9.2
IA-2(13)	Implement the following out-of-band authentication mechanisms under [*Assignment: organization-defined conditions*]: [*Assignment: organization-defined out-of-band authentication*].	• 800-63B-4 Table 1, Section 5.1.3 and subsections; 10.2.3; 11 • 800-63C-4 Section 6.1.2.2
IA-3	Uniquely identify and authenticate [*Assignment: organization-defined devices and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.	Not Applicable – NIST 800-63 scope is limited to identity proofing and authentication of users (such as employees, contractors, or private individuals); devices are out of scope.
IA-3(1)	Authenticate [*Assignment: organization-defined devices and/or types of devices*] before establishing [*Selection (one or more): local; remote; network*] connection using bidirectional authentication that is cryptographically based.	Not Applicable – NIST 800-63 scope is limited to identity proofing and authentication of users (such as employees, contractors, or private individuals); devices are out of scope.
IA-3(3)	(a) Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [*Assignment: organization-defined lease information and lease duration*]; and	Not Applicable – NIST 800-63 scope is limited to identity proofing and authentication of users (such as employees, contractors, or private individuals); devices are out of scope.

Control	NIST SP 800-53 R5 Control	NIST SP 800-63 (Draft Version 4) Guidance
	(b) Audit lease information when assigned to a device.	
IA-3(4)	Handle device identification and authentication based on attestation by [*Assignment: organization-defined configuration management process*].	Not Applicable – NIST 800-63 scope is limited to identity proofing and authentication of users (such as employees, contractors, or private individuals); devices are out of scope.
IA-4	Manage system identifiers by: a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, service, or device identifier;	No direct mapping. However, see 800-63A-4 Sections 4.3.4.4, 5.1.1
	b. Selecting an identifier that identifies an individual, group, role, service, or device;	• 800-63A-3 Sections 2.1, 4 and subsections, 6.1, Table 1
	c. Assigning the identifier to the intended individual, group, role, service, or device; and	• 800-63A-3 Sections 2.1, 4 and subsections 6.1, Table 1
	d. Preventing reuse of identifiers for [Assignment: organization-defined time period].	• 800-63B-4 Section 4
IA-4(1)	Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.	None
IA-4(4)	Manage individual identifiers by uniquely identifying each individual as [*Assignment: organization-defined characteristic identifying individual status*].	No direct mapping. However, see 800-63A-3 Section 6.1
IA-4(5)	Manage individual identifiers dynamically in accordance with [*Assignment: organization-defined dynamic identifier policy*].	• 800-63C-4 Section 5.2 and subsections
IA-4(6)	Coordinate with the following external organizations for cross-organization management of identifiers: [*Assignment: organization-defined external organizations*].	• 800-63C-4 Section 6.3.1
IA-4(8)	Generate pairwise pseudonymous identifiers.	• 800-63-4 Section 4.4.1 • 800-63B-3 Section 4 • 800-63C-4 Sections 5.2.2, 5.5, 6.2.5 and subsections, 9.1, 9.2
IA-4(9)	Maintain the attributes for each uniquely identified individual, device, or service in [*Assignment: organization-defined protected central storage*].	• 800-63-4 Sections 2.3.1, 4.3.2 • 800-63A-4 Section 5.1.4 • 800-63C-4 Sections 5.4.2, 6.3.1

Control	NIST SP 800-53 R5 Control	NIST SP 800-63 (Draft Version 4) Guidance
IA-5	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;	• 800-63-4 Sections 2.1, 4.2, 5.0, 5.1 and subsections, 5.2.2.1, 5.2.3.1, 5.3 and subsections, Figures 1 & 2 • 800-63B-4 Sections 2 and subsections, 4 and subsections, 5 and subsections. Suggest reading other sections as well for full context/insight.
	b. Establishing initial authenticator content for any authenticators issued by the organization;	None. However, see 800-63B-4 Section 6.1 and subsections
	c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;	• 800-63-4 Sections 5.0, 5.1 and subsections, 5.2.2.2, 5.2.3.2, 5.3 and subsections, • 800-63B-4 Section 4 and subsections, 5 and subsections. Suggest reading other sections as well for full context/insight.
	d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;	• 800-63-4 Sections 5.2.1, 5.2.2.2, 5.2.3.2, 5.3 and subsections • 800-63B-4 Section 6 and subsections
	e. Changing default authenticators prior to first use;	None
	f. Changing or refreshing authenticators [*Assignment: organization-defined time period by authenticator type*] or when [*Assignment: organization-defined events*] occur;	• 800-63B-4 Sections 6.1.4, 6.2, 6.3
	g. Protecting authenticator content from unauthorized disclosure and modification;	• 800-63B-4 Sections 4.1.4, 4.2.4, 4.3.4, 5.1 and subsections, 5.2.1, 5.2.3, 6.1, 6.1.1, 6.1.2.4
	h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and	• 800-63B-3 Section 5.2.1
	i. Changing authenticators for group or role accounts when membership to those accounts changes.	None
IA-5(1)	For password-based authentication: (a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [*Assignment: organization-defined frequency*] and when organizational passwords are suspected to have been compromised directly or indirectly;	• 800-63B-4 Sections 5.1.1 and subsections, See also Section 10.2.1 and Appendix A for general discussion
	(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);	• 800-63B-4 Section 5.1.1 and subsections

Control	NIST SP 800-53 R5 Control	NIST SP 800-63 (Draft Version 4) Guidance
	(c) Transmit passwords only over cryptographically-protected channels;	• 800-63B-4 Section 5.1.1 and subsections
	(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;	• 800-63B-4 Section 5.1.1 and subsections, Table 4
	(e) Require immediate selection of a new password upon account recovery;	• 800-63B-4 Section 6.1.2.3, 8.3
	(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;	• 800-63B-4 Section 5.1.1 and subsections
	(g) Employ automated tools to assist the user in selecting strong password authenticators; and	• 800-63B-4 Sections 5.1.1 and subsections
	(h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	• 800-63B-4 Section 5.1.1 and subsections
IA-5(2)	(a) For public key-based authentication: (1) Enforce authorized access to the corresponding private key; and	• 800-63B-4 Section 5.1.6.1, 5.1.7.1, 5.1.8.1
	(2) Map the authenticated identity to the account of the individual or group; and	• 800-63A-3 Sections 2.1, 4 and subsections, 6.1, Table 1
	(b) When public key infrastructure (PKI) is used: (1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and (2) Implement a local cache of revocation data to support path discovery and validation.	None
IA-5(5)	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.	Not Applicable
IA-5(6)	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	• 800-63-4 Section 5 and subsections • 800-63B-4 Sections 4.1.4, 4.2.4, 4.3.4, 5.2.1
IA-5(7)	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.	None. However, see the following regarding authenticator storage: 800-63B-4 Sections 5.1.1.2, 5.1.2.2, 5.1.3.1, 5.1.3.2, 5.1.6.1, 5.1.8.1, 5.2.7, 5.2.11
IA-5(8)	Implement [*Assignment: organization-defined security controls*] to manage the risk of compromise due to individuals having accounts on multiple systems.	• 800-63-4 Section 4.4 • 800-63C-4 for overall guidance on Federation / SSO
IA-5(9)	Use the following external organizations to federate credentials: [*Assignment: organization-defined external organizations*].	None. This is a case-by-case decision; see 800-63C-4 for overall guidance on Federation and collaborating and coordinating with external entities.
IA-5(10)	Bind identities and authenticators dynamically using the following rules: [*Assignment: organization-defined binding rules*].	• 800-63B-4 Sections 6.1.2.4, 6.1.3

Control	NIST SP 800-53 R5 Control	NIST SP 800-63 (Draft Version 4) Guidance
IA-5(12)	For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [*Assignment: organization-defined biometric quality requirements*].	• 800-63B-4 Section 5.1.8
IA-5(13)	Prohibit the use of cached authenticators after [*Assignment: organization-defined time period*].	None
IA-5(14)	For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.	None
IA-5(15)	Use only General Services Administration-approved products and services for identity, credential, and access management.	None
IA-5(16)	Require that the issuance of [*Assignment: organization-defined types of and/or specific authenticators*] be conducted [*Selection: in person; by a trusted external party*] before [*Assignment: organization-defined registration authority*] with authorization by *[Assignment: organization-defined personnel or roles*].	• 800-63-4 Section 4.2 • 800-63A-4 Section 9.3, 9.4 • 800-63B-4 Sections 6.1 and subsections • 800-63C-4 Sections 6.1.2.2
IA-5(17)	Employ presentation attack detection mechanisms for biometric-based authentication.	• 800-63-A-4 Table 3, Sections 5.1.1, 5.3.4, 5.4.4, 5.5.4 • 800-63B-4 Section 5.2.3
IA-5(18)	(a) Employ [*Assignment: organization-defined password managers*] to generate and manage passwords; and	• 800-63B-4 Section 5.1.1.2, 5.1.2.2, 5.1.1.4
	(b) Protect the passwords using [*Assignment: organization-defined controls*].	• 800-63B-4 Section 5.1.1.2, 5.1.2.2, 5.1.1.4 • 800-63C-4 Section 12.2
IA-6	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	• 800-63B-4 Section 5.1.1.2
IA-7	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	• 800-63-4 Section 2.3.1 • 800-63B-4 Section 4, 4.3.2, 5.1.5, 5.1.8, 5.1.9, 5.1.7.1, 5.1.9.1, Table 1
IA-8	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	• 800-63-4 Section 2.1, 4 and subsections, Appendix A.1 (Federated Identifier, Identity, Identity Resolution) • 800-63A-4 Section 4 and subsections, Section 5 and subsections. However, best to read 800-63A-4 in full • 800-63B-4 Sections 4 and subsections and 5 and subsections. However, best to read 800-63B-4 in full

Control	NIST SP 800-53 R5 Control	NIST SP 800-63 (Draft Version 4) Guidance
		• 800-63C-4 Sections 4 and subsections and 5 and subsections. However, best to read 800-63C-4 in full
IA-8(1)	Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.	No direct mapping. However, see 800-63A-4 Sections 4.4, 4.4.1, and 800-63C-4 for information regarding sharing with other federal agencies. See also OMB Memo dated 10/6/2011, *Requirements for Accepting Externally Issued Identity Credentials*.
IA-8(2)	(a) Accept only external authenticators that are NIST-compliant; and	• 800-63-4 Section 2.3.1 • 800-63A-4 Sections 4.3.2 (6), 5.3.4, 5.5.4 • 800-63B-4 Section 4 and subsections, 5 and subsections, 6.1.2.4
	(b) Document and maintain a list of accepted external authenticators.	• 800-63A-4 Sections 2, 5, 5.1.5, 6.1, 6.3.1, 7.2
IA-8(4)	Conform to the following profiles for identity management [*Assignment: organization-defined identity management profiles*].	• 800-63-4 Sections 4.4, 4.4.2, References section • 800-63A-4 References section • 800-63B-4 References section • 800-63C-4 Sections 4, 4.1, 4.2, 4.3, 5.1.2, 6.2.3, 6.3, 10.2, 10.2.2, 12 and subsections, References section
IA-8(5)	Accept and verify federated or PKI credentials that meet [*Assignment: organization-defined policy*].	None. However, see 800-63A-4 Sections 4.4, 4.4.1, and 800-63C-4 for information regarding accepting external credentials.
IA-8(6)	Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: [*Assignment: organization-defined measures*].	• 800-63-4 Sections 2.3.2, 5.5 • 800-63A-4 Section 5.1.2.1 • 800-63B-4 Sections 4.9.2, 4.9.3, 4.9.4 • 800-63C-4 Sections 5.5, 6.2.4, 6.2.5 and subsections, 6.3, 9.1
IA-9	Uniquely identify and authenticate [*Assignment: organization-defined system services and applications*] before establishing communications with devices, users, or other services or applications.	• 800-63B-4 Sections 4.1.2, 4.2.2, 4.3.2, Table 1, 5.1.2.2, 5.1.4.2, 5.1.5.2, 5.2.5, 5.2.5.1, 5.2.5.2, 7.1.3 (Devices), Table 4
IA-10	Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].	• 800-63B-4 Section 5.2.2
IA-11	Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	• 800-63B-4 Sections 4.1.3, 4 4.2.3, 4.3.3, 4 7.2
IA-12	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;	• 800-63-4 Sections 4.2, 4.3.2, 5 and subsections • 800-63A-4 Section 4 and subsections, 5 and subsections

Control	NIST SP 800-53 R5 Control	NIST SP 800-63 (Draft Version 4) Guidance
	b. Resolve user identities to a unique individual; and	• 800-63A-4 Sections 2, 2.1, 4.1 and subsections, 4.2, 4.3.3.1, 4.3.3.2, 4.3.3.3, 5.1.8, 6.1, 6.3.1 • 800-63C-4 Sections 2, 6
	c. Collect, validate, and verify identity evidence.	• 800-63A-4 Section 4 and subsections, 5.1.8, 5.1.9 and subsections, 5.1.10, 5.2, 5.3 and subsections, 5.4 and subsections, 5.5 and subsections, Table 1, 7 and subsections
IA-12(1)	Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.	No direct mapping. However, see 800-63A-4 Section 5.2.2.1 for authorization around identity attributes.
IA-12(2)	Require evidence of individual identification be presented to the registration authority.	• 800-63-4 Sections 5.2.2.1, 5.3.2, 5.3.3
IA-12(3)	Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].	• 800-63A-4 Sections 4.3, 4.4
IA-12(4)	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	• 800-63A-4 Sections 4.3.4.3, 4.4.1, 5.3.2, 5.5.7
IA-12(5)	Require that a [Selection: registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.	• 800-63A-4 Sections 5.1.6, 5.1.7
IA-12(6)	Accept externally-proofed identities at [Assignment: organization-defined identity assurance level].	• 800-63C-4 Section 4

Policy Crosswalk

Policy crosswalk overview Table

This table presents a high-level summary of the relationship of controls in 800-53 to sections in the 800-63 set of documents. Because we are mapping between requirements in each document, only the *normative* sections of 800-63 are included in the mapping. Informative sections are excluded.

Empty, light-gray cells identify controls for which none of the sections can be directly mapped.

When a section appears with an asterisk (*), this indicates that the reference includes the subsections as well as the section itself.

800-53 Control	800-63 Section	800-63A Section	800-63B Section	800-63c Section
IA-1 a.1 (a)	5.1.2, 5.3.2, 5.3.3, 5.5	5.1.5		5.1, 5.1.1, 5.1.2
IA-1 a.1 (b)	5	4.3.3.3, 5.1.2.1, 5.1.4, 5.1.5, 5.1.8, 5.1.10	4., 4.1.2, 4.1.4, 4.1.5, 4.2.2, 4.2.4, 4.2.5, 4.3.2, 4.3.4, 4.3.5, 4.4, 5.1.1.2, 5.1.2.1, 5.1.3.2, 5.1.4.1, 5.1.5.1, 5.1.7.1, 5.1.9.1, 5.2.3, 5.2.4, 5.2.5, 5.2.12, 6.1.2.3, 7.1	4, 4.2, 4.3,
IA-1 a. 2	5.2.3, 5.3	5.1.1, 5.1.10		
IA-1 b				
IA-1 c.1 IA-1 c.2				
IA-2		6.1	Internal Users: 4 CSPs: 6.1	
IA-2(1)				
IA-2(2)				
IA-2(5)				
IA-2(6)				
IA-2(6)(a)			4.2.1, 4.3.1, 5.1.9.1	
IA-2(6)(b)			4.2.2,, 4.3.2	
IA2(8)			4.2.2, 4.3.2, 5.1.3.2, 5.1.4.2, 5.1.5.2	
IA-2(10)				
IA-2(12)				
IA-2(13)			5.1.3*, 5.2.5	

Commented [1]: There is no specific requirement in 800-63 related to privileged vs. non-privileged accounts.

Commented [2]: This requirement is unique to shared accounts or authenticators, which are not addressed in 800-63

Commented [3]: This statement is broken out below, and the sub-requirements are addressed individually.

800-53 Control	800-63 Section	800-63A Section	800-63B Section	800-63c Section
IA-3				
IA-4 a.				
IA-4 b.		6.1		5.4, 5.4.1
IA-4 c.		6.1		5.4, 5.4.1
IA-4 d.			4.	
IA-4(1)				
IA-4(4)				
IA-4(5)				5.4.1
IA-4(6)				5.1, 5.1.2
IA-4(8)				5.5, 6.2.5*
IA-4(9)		6.1		5.4.2, 6.3.1
IA-5 a.	5.2.1	4.4.1, 5.3.4, 5.4.4*, 5.5.4, 5.5.7		
IA-5 b.				
IA-5 c.	5.2.1		This is a generic requirement, which is addressed by most of sections 4*, 5*	
IA-5 d.			Details of potential procedures to satisfy this requirement are contained in 6*	
IA-5 e.				
IA-5 f.			6.1.4	
IA-5 g.			4.1.2, 4.1.4, 4.2.2, 4.2.4, 4.3.2, 4.3.4, 5.1.1.2, 5.1.2.1, 5.1.2.2, 5.1.3.1, 5.1.3.3, 5.1.3.4,	

800-53 Control	800-63 Section	800-63A Section	800-63B Section	800-63c Section
			5.1.4.2, 5.1.5.1, 5.1.5.2, 5.1.6.1, 5.1.7.1, 5.1.7.2, 5.1.8.1, 5.1.9.1, 5.2.1, 5.2.3, 5.2.11, 5.2.12, 6.1, 6.1.1	
IA-5 h.			4.1.2, 4.2.2, 5.1.3.1, 5.1.3.4, 5.1.5.1, 5.1.6.1, 5.1.7.1, 5.1.8.1, 5.1.9.1, 5.2.1, 5.2.12,	
IA-5 i.				
IA-5 (1) (a)			5.1.1*	
IA-5 (1) (b)			5.1.1.2	
IA-5 (1) (c)			5.1.1.2	
IA-5 (1) (d)			5.1.1.2	
IA-5 (1) (e)			6.1.2.3	
IA-5 (1) (f)			5.1.1.2	
IA-5 (1) (g)			5.1.1.2	
IA-5 (1) (h)			5.1.1.1, 5.1.1.2	
IA-5 (2) (a) (1)			5.1.6.1, 5.1.7.1, 5.1.8.1, 5.1.9.1	
IA-5 (2) (a) (2)		6.1	6.1, 6.1.1	
IA-5 (2) (b)				
IA-5 (5)				
IA-5 (6)			4.1.4, 4.2.4, 4.3.4, 5.2.1	
IA-5 (7)				
IA-5 (8)				

800-53 Control	800-63 Section	800-63A Section	800-63B Section	800-63c Section
IA-5 (9)				
IA-5 (10)			6.1.2.4, 6.1.3	
IA-5 (12)			5.2.3	
IA-5 (13)				
IA-5 (14)				
IA-5 (15)				
IA-5 (16)			6.1, 6.1.1	6.1.2.2
IA-5 (17)			5.2.3	
IA-5 (18) (a)/(b)			5.1.1.2	
IA-6			5.1.1.2	
IA-7			5.1.7.1, 5.1.8, 5.1.9, 5.1.9.1	
IA-8		6.1	4	5.4, 6, 6.2.5.1
IA-8 (1)				
IA-8 (2) (a)		4.3.2, 5.3.4, 5.4.4.1, 5.5.4	4, 4.1.1, 4.2.1, 4.3, 4.3.1	
IA-8 (2) (b)	5.1.2, 5.2.3, 5.2.3.2	5.1.5		5.1, 5.1.1
IA-8 (4)			5.2.7	4, 4.1, 4.2, 4.3, 5.1.2
IA-8 (5)				
IA-8 (6)		5.1.2.1	4.	5.5, 6.2.5*
IA-9			4.1.2, 5.2.5.2	
IA-10			5.2.2	
IA-11			4.1.3, 4.2.3, 4.3.3, 7.2	
IA-12 a.	5.2.3.1	4.4.1, 5.3.2.1, 5.3.4, 5.4.4*, 5.5.4, 5.5.7, 5.5.8,		4.4

Commented [4]: "Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies."

Commented [5]: "Accept and verify federated or PKI credentials that meet [Assignment: organization-defined policy]."

800-53 Control	800-63 Section	800-63A Section	800-63B Section	800-63c Section
IA-12 b.		5.1.2.2		6, 6.2.5.1
IA-12 c.		4.3, 4.3.1, 4.3.2, 4.3.3*, 4.3.4*, 5.3.3, 5.4.2*, 5.4.3, 5.5.2.1, 5.5.3*, 5.5.4		
IA-12 (1)				
IA-12 (2)		4.4.1, 5.3.2.1, 5.4.2.1, 5.5.7, 5.5.8		
IA-12 (3)		4.3.3*, 4.3.4, 4.3.4.1, 5.5.8		
IA-12 (4)		4.4.1, 5.5.7		
IA-12 (5)		5.1.6, 5.1.7		
IA-12 (6)				4.4

Detailed Policy Crosswalk

800-63-4

NIST 800-63 Reference	800-53 rev 5 control
1. Purpose (Informative)	
2. Introduction (Informative)	
3. Definitions and Abbreviations (Informative)	
4. Digital Identity Model (Informative)	
5. Digital Identity Risk Management	
Organizations **SHOULD** adapt and modify this overall approach to meet organizational processes, governance, and integration with	IA-1 a.1 (b)

NIST 800-63 Reference	800-53 rev 5 control
enterprise risk management practices.	
At a minimum, organizations **SHALL** ensure that each step is executed and the normative mandates and outcomes of each step are completed and documented regardless of operational approach and enabling tools.	IA-1 a.1 (b)
5.1 Conduct Initial Impact Assessment	
5.1.1. Identify Impacted Entities	
Accordingly, impact assessments **SHALL** include individuals using the system or application in addition to the organization itself.	
Additionally, organizations **SHOULD** identify other entities, such as mission partners, communities, and those identified in [SP800-30], that need to be specifically included based on mission and business needs.	
At a minimum, agencies **SHALL** document all entities to which impacts will be assessed when conducting their impact analysis.	
5.1.2. Identify Impact Categories and Potential Harms	
Initial assurance levels for digital transactions **SHALL** be determined by assessing the potential impact of, at a minimum, each of the following categories: ● Damage to mission delivery ● Damage to trust or reputation ● Loss of sensitive information ● Damage to or loss of economic stability ● Loss of life or damage to safety, health, or environmental stability ● Noncompliance with laws, regulations, and/or contractual obligations	IA-8 (2) (b)
Organizations **SHOULD** include additional impact categories as appropriate based on their mission.	
Each impact category **SHALL** be documented and consistently applied across different applications assessed by the organization.	IA-1 a.1 (a), IA-8 (2) (b)

NIST 800-63 Reference	800-53 rev 5 control
Agencies **SHOULD** consider specific harms for each of the defined impact categories to better inform their impact analysis.	
Identification of harms for each category **SHALL** be done for each of the entities identified during "entity identification" process.	IA-1 a.1 (a)
5.1.3. Identify Potential Impact Levels	
Each assurance level, IAL, AAL, and FAL (if accepting or asserting a federated identity) **SHALL** be evaluated separately. Ideally, any evaluation will include different viewpoints such as harm to individuals, the organization, other organizations, and the nation as applicable to successful delivery of the organization's mission.	
5.1.4. Impact Analysis	
To determine the appropriate level of assurance of the user's asserted identity, organizations **SHALL** assess the potential risks and identify measures to minimize their impact.	
Organizations **SHALL** assess the risk of identity proofing, authentication, and federation failures separately to determine the required assurance level for each transaction.	
This process **SHALL** include consideration of potentially varying impacts of harms to different entities impacted by the digital identity system, as described in Sec. 5.1.1.	
Entities **SHOULD** consider the impact of specific modes of failures related to identity proofing, authentication, and federation	
5.2. Select Initial Assurance Levels	
5.2.1. Assurance Levels	
An organization RP **SHALL** select, based on cybersecurity risk and mission needs, the following individual initial assurance levels: • **IAL**: The robustness of the identity proofing process to confidently determine the identity of an individual. IAL is selected to mitigate potential identity proofing failures.	IA-5 a. IA-5 c.

NIST 800-63 Reference	800-53 rev 5 control
• **AAL**: The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier. AAL is selected to mitigate potential authentication failures. • **FAL**: The robustness of the federation process used to communicate authentication and attribute information (if applicable) to an RP from an IdP. FAL is optional as not all digital systems will leverage federated identity architectures. FAL is selected to mitigate potential federation failures.	
5.2.2. xAL Descriptions	
5.2.2.1. Identity Assurance Level	
5.2.2.2. Authentication Assurance Level	
5.2.2.3. Federation Assurance Level	
5.2.3 Initial Assurance Level Selection	
Organizations **SHALL** develop and document a process and governance model for selecting initial assurance levels based on the potential impact of digital identity failures. This section provides guidance on the major elements to include in that process.	IA-1 a. 2, IA-8 (2) (b)
5.2.3.1. Selecting Initial IAL	
Organizations **SHALL** use a risk-based approach to select the most appropriate identity proofing requirements for their RP application.	IA-12 a.
This initial selection **SHALL** be tailored, as described in Sec. 5.3, based on mission needs, risk tolerance, and potential impacts to privacy, equity, and usability, before making a final IAL determination.	IA-12 a.
If an organization determines that identity proofing is necessary, the initial IAL **SHALL** be assessed based on the potential impacts of identity proofing failures.	IA-12 a.
If an organization determines that identity proofing is necessary, the initial IAL **SHALL** be assessed based on the potential impacts of	IA-12 a.

NIST 800-63 Reference	800-53 rev 5 control
identity proofing failures.	
As described in Sec. 5.1, potential impacts **SHALL** be considered from the perspective of the organization, individuals, other organizations, and the nation, for harms incurred through the use or operation of the RP application.	IA-12 a.
Organizations **SHOULD** consider the worst-case when identifying the overall impact level of the RP application, but may use risk management processes to tailor their initial selection when there are differing impacts.	IA-12 a.
When assessing the overall impact level of the RP application, the organization **SHOULD** consider impacts to mission delivery separately from other impact categories.	IA-12 a.
As such, the organization **MAY** exclude the mission delivery category when initially identifying the overall impact level of the RP application, as these impacts will need to be considered in the tailoring process.	IA-12 a.
5.2.3.2. Selecting Initial AAL	
Organizations **SHALL** use a risk-based approach to select the most appropriate authentication requirements for their RP application.	IA-8 (2) (b)
This initial selection **SHALL** be tailored, as described in Sec. 5.3, based on mission needs, risk tolerance, and potential impacts to privacy, equity, and usability, before making a final AAL determination.	IA-8 (2) (b)
The initial AAL **SHALL** be assessed based on the potential impacts of authentication failures.	IA-5 (6), IA-8 (2) (b)
As described in Sec. 5.1, potential impacts **SHALL** be considered from the perspective of the organization, individuals, other organizations, and the nation, for harms incurred through the use or operation of the RP application, as the level of harm from a failure could vary significantly across these entities.	IA-8 (2) (b)

NIST 800-63 Reference	800-53 rev 5 control
Organizations **SHOULD** consider the worst-case when identifying the overall impact level of the RP application, but may use risk management processes to tailor their initial selection when there are differing impacts.	IA-8 (2) (b)
When assessing the overall impact level of the RP application, the organization **SHOULD** consider impacts to mission delivery separately from other impact categories.	IA-8 (2) (b)
As such, the organization **MAY** exclude the mission delivery category when initially identifying the overall impact level of the RP application, as these impacts will need to be considered in the tailoring process.	IA-8 (2) (b)
5.2.3.3. Selecting Initial FAL	
Organizations **SHALL** use a risk-based approach to select the most appropriate federation requirements for their RP application.	
This initial selection **SHALL** be tailored, as described in Sec. 5.3, based on mission needs, risk tolerance, and potential impacts to privacy, equity, and usability, before making a final FAL determination.	
The initial FAL **SHALL** be assessed based on the potential impacts of failures in the presentation or acceptance of assertions in federated identity architectures.	
As described in Sec. 5.1, potential impacts **SHALL** be considered from the perspective of the organization, individuals, other organizations, and the nation, for harms incurred through the use or operation of the RP application, as the level of harm from a failure could vary significantly across these entities.	
Organizations **SHOULD** consider the worst-case when identifying the overall impact level of the RP application, but may use risk management processes to tailor their initial selection when there are differing impacts.	
When assessing the overall impact level of the RP application, the	

NIST 800-63 Reference	800-53 rev 5 control
organization **SHOULD** consider impacts to mission delivery separately from other impact categories.	
Potential failures in federated architectures that could lead to harms in mission delivery **MAY** be assessed by the organization to determine if the associated impacts would be mitigated or exacerbated by the implementation of more rigorous controls by identity providers.	
5.3. Tailor and Document Assurance Levels	
Organizations **SHOULD** implement the assessed assurance level as defined in these guidelines.	
Therefore, organizations **SHALL** establish and document an xAL tailoring process.	IA-1 a. 2
At a minimum this process: 1. **SHALL** include a structured governance approach to allow for decision-making and conflict resolution. 2. **SHALL** document all decisions in the tailoring process, including the assessed xALs, modified xALs, and compensating controls in the Digital Identity Acceptance Statement (see Sec. 5.3.4). 3. **SHALL** justify and document all risk-based decisions or modifications to the initially assessed xALs in the Digital Identity Acceptance Statement (see Sec. 5.3.4). 4. **SHOULD** establish a cross-functional capability to support subject matter analysis of xAL selection impacts in the tailoring process. 5. **SHOULD** be a continuous process that incorporates real world operational data to evaluate the impacts of selected xAL controls.	IA-1 a. 2
5.3.1. Assess Privacy, Equity, Usability and Threats	
When transitioning from an initial assurance level to the final xAL selection and implementation, organizations **SHALL** conduct detailed assessments of the controls defined at the assurance level to determine potential impacts in their operational environment.	

NIST 800-63 Reference	800-53 rev 5 control
At a minimum, organizations **SHALL** assess impacts related to the following areas: • **Privacy** – to determine unintended consequences to the privacy of individuals that will be subject to the controls at an assessed xAL and of individuals affected by organizational or third-party practices related to the establishment, management, or federation of a digital identity. • **Equity** – to determine whether implementation of controls may create or maintain inequities across demographics or user groups. • **Usability** – to determine whether implementation of the selected controls will result in challenges to end-user experience. • **Threat** – to determine whether the defined assurance level will address specific threats based on environment, threat actors, and known tactics, techniques, and procedures (TTPs).	
Additionally, organizations **SHOULD** conduct additional business specific assessments as appropriate to fully represent mission and domain specific considerations not captured here.	
These assessments **SHALL** be extended to any compensating or supplemental controls as defined in Sec. 5.3.2 and Sec. 5.3.3.	
5.3.2. Identify Compensating Controls	
Organizations **SHOULD** implement their identity services per the requirements in these guidelines for their tailored assurance level. However, where organizations are unable to implement a specific control associated with their baseline or tailored assurance level, they **MAY** select to implement a compensating control.	
This control **MAY** be a modification to a digital identity process as defined in these guidelines, but **MAY** also be applied elsewhere in an application, transaction, or service lifecycle.	
Where compensating controls are implemented, organizations **SHALL** demonstrate comparability of a chosen alternative or document residual risk incurred by deviating from normative	

NIST 800-63 Reference	800-53 rev 5 control
requirements.	
Organizations **SHALL** implement procedures to document both the justification for any departure from normative requirements and detail the compensating controls employed.	IA-1 a.1 (a)
5.3.3. Identify Supplemental Controls	
Organizations **SHOULD** identify and implement supplemental controls where they identify threats that may not be addressed in baseline controls.	
Where organizations implement supplemental controls, these **SHALL** be assessed for impacts based on the same factors used to tailor the organization's assurance level.	
Supplemental controls **SHALL** be documented.	IA-1 a.1 (a)
5.3.4. Document Results - The Digital Identity Acceptance Statement	
The statement **SHALL** include, at a minimum: 1. Initial Impact Assessment Results 2. Initially assessed xAL, 3. Tailored xAL and rationale, if tailored xAL differs from initially assessed xAL, 4. All compensating controls and their comparability or residual risk associated with compensating controls 5. All supplemental controls	
Federal agencies **SHOULD** include this information in the system authorization package described in [SP800-37].	
5.4. Continuously Evaluate and Improve	
To maintain pace with the constantly shifting environment in which they operate, organizations **SHOULD** implement a continuous evaluation and improvement program that leverages input from people interacting with the identity system.	

NIST 800-63 Reference	800-53 rev 5 control
These programs **SHOULD** consider feedback from application performance metrics, threat intelligence, fraud analytics, assessments of equity impacts, privacy impact analysis, and user inputs.	
5.5. Cyber, Fraud, and Identity Program Integrity	
Organizations **SHOULD** establish consistent mechanisms for the exchange of information between critical security and fraud stakeholders.	IA-1 a. 1. (a)
Where supporting service providers, such as CSPs, are external, this may be complicated, but **SHOULD** be considered in contractual and legal mechanisms.	
All data collected, transmitted, or shared **SHALL** be minimized and subject to a detailed privacy and legal assessment.	

800-63A-4

NIST 800-63A Reference	800-53 rev 5 control
1. Purpose (Informative)	
2. Introduction (Informative)	
3. Definitions and Abbreviations (Informative)	
4. Identity Resolution, Validation, and Verification	
To the extent practical, CSPs and organizations SHOULD enable optionality when implementing their identity proofing services and processes to promote access for those with different means, capabilities, and technology access.	
At a minimum, this **SHOULD** include accepting multiple types and combinations of identity evidence, supporting multiple data validation sources, enabling multiple methods for verifying identity	

(e.g., use of trusted referees), multiple channels for engagement (e.g., in-person, remote), and offering assistance mechanisms for applicants (e.g., applicant references).	
4.1. Identity Proofing and Enrollment	
4.1.1. Identify Impacted Entities	
4.2. Identity Resolution	
4.3. Identity Validation and Identity Evidence Collection	
The CSP **SHALL** determine the acceptability of presented identity evidence for identity proofing based on the evidence characteristics in this section.	IA-12 c.
4.3.1. Characteristics of Acceptable Physical Evidence	
Acceptable physical evidence **SHALL** contain all of the following characteristics: ● The presented document contains the printed name of the applicant. (See Sec. 10.1 - Equity and Resolution - for guidance on dealing with a printed name that varies from the applicant's claimed identity.) ● The presented document contains at least one printed reference number. ● The presented document contains the printed name of the issuer of the document. ● The issuer of the document performed identity proofing of the applicant prior to issuing the document. ● There is reasonable assurance that the document was delivered to the intended person.	IA-12 c. IA-12 (3)
4.3.2. Characteristics of Acceptable Digital Evidence	
Acceptable digital evidence **SHALL** contain all of the following characteristics: 1. The presented digital evidence contains the name of the applicant as the subject of the digital information or account. (See Sec. 10.1 - Equity and Resolution - for guidance on dealing with a name on digital evidence that varies from the applicant's claimed identity.) 2. The presented digital evidence contains at least one	IA-12 c. IA-12 (3) IA-8 (2) (a)

reference (e.g., account number) or sufficient attributes to bind the digital information to the applicant. 3. The presented digital evidence contains the name of the issuer of the digital information. 4. The issuer of the digital evidence performed identity proofing of the applicant prior to issuing the digital evidence. 5. There is reasonable assurance that the digital evidence was delivered or made accessible to intended person. 6. If applicable, the presented digital evidence can be verified through authentication at an AAL or FAL commensurate with the assessed IAL	
4.3.3. Evidence Strength Requirements	
4.3.3.1. Fair Evidence Requirements	
In order to be considered FAIR, identity evidence **SHALL** meet *all* the following requirements: 1. The issuing source of the evidence confirmed the claimed identity through an identity proofing process. 2. It can be reasonably assumed that the evidence issuing process would result in the delivery of the evidence to the person to whom it relates. 3. The evidence contains at least one reference number, a facial portrait, or sufficient attributes to uniquely identify the person to whom it relates. 4. The evidence has not expired or it expired within the previous six (6) months, or it was issued within the previous six (6) months if it does not contain an expiration date.	IA-12 c. IA-12 (3)
4.3.3.2. Strong Evidence Requirements	
In order to be considered STRONG, identity evidence **SHALL** meet *all* the following requirements: 1. The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures are subject to recurring oversight by regulatory or publicly-accountable institutions. For example, the Customer Identification Program guidelines established in response to the USA PATRIOT Act of 2001 or the [RedFlagsRule], under Sec. 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act).	IA-12 c. IA-12 (3)

2. There is a high likelihood that the evidence issuing process would result in the delivery of the evidence to the person to whom it relates. 3. The evidence contains a reference number or other attributes that uniquely identify the person to whom it relates. 4. The evidence contains a facial portrait or other biometric characteristic of the person to whom it relates. 5. The evidence includes physical security features that make it difficult to copy or reproduce. 6. The evidence includes an expiration date and is unexpired.	
4.3.3.3. Superior Evidence Requirements	
In order to be considered SUPERIOR, identity evidence **SHALL** meet *all* the following requirements: 1. The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. 2. The issuing source visually identified the applicant and performed further checks to confirm the existence of that person. 3. The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates. 4. The evidence contains at least one reference number that uniquely identifies the person to whom it relates. 5. The evidence contains a facial portrait or other biometric characteristic of the person to whom it relates. 6. The evidence includes digital information that is cryptographically signed. 7. The evidence includes physical security features that make it difficult to copy or reproduce. 8. The evidence includes an expiration date and is unexpired.	IA-12 c. IA-12 (3)
4.3.4. Identity Evidence and Attribute Validation	
The CSP **SHALL** validate all identity evidence collected to meet evidence collection requirements and all core attribute information required by the CSP identity service.	IA-12 c., IA-12 (3)

4.3.4.1. Evidence Validation	
The CSP **SHALL** validate the authenticity, accuracy, and currency of presented evidence by: ● Confirming the evidence is in the correct format and includes complete information for the identity evidence type. ● Confirming the evidence is not counterfeit and that it as not been tampered with. ● Confirming any security features.	IA-12 c., IA-12(3)
The CSP **SHALL** validate that the evidence is current through confirmation that its expiration date has not passed or that evidence without an expiration date was issued within the previous six (6) months.	IA-12 c., IA-12(3)
The CSP **SHALL** use the public key of the issuing authority of the evidence to verify digitally signed evidence or attribute data objects.	IA-12 c., IA-12(3)
4.3.4.2 Attribute Validation	
4.3.4.3. Evidence and Attribute Validation Methods	
4.3.4.4. Validation Sources	
4.4. Identity Verification	
4.4.1. Identity Verification Methods	
The CSP **SHALL** verify the linkage of the claimed identity to the applicant engaged in the identity proofing process through one or more of the following methods, depending on the IAL identity verification requirements presented in Sec. 5. ● **Enrollment code verification** as specified in Sec. 5.1.6. ● **In-person physical comparison**. The CSP operator and applicant interact in person for the identity proofing event. The CSP operator performs a physical comparison of the facial portrait presented on identity evidence to the face of the applicant engaged in the identity proofing event. ● **Remote (attended and unattended) physical facial image comparison**. The CSP operator performs a physical comparison of the facial portrait presented on identity evidence to the facial image of the applicant engaged in the	IA-5 a., IA-12 a., IA-12 (2), IA-12 (4)

identity proofing event. The CSP operator may interact directly with the applicant during some or all of the identity proofing event (attended) or may conduct the comparison at a later time (unattended) using a captured video or photograph and the uploaded copy of the evidence. If the comparison is performed at a later time, steps are taken to ensure the captured video or photograph was taken from the live applicant present during the identity proofing event. ● **Automated biometric comparison**. Biometric system comparison may be performed for in-person or remote identity proofing events. The facial portrait, or other biometric characteristic, contained on identity evidence is compared by an automated biometric comparison system to the facial image photograph of the live applicant or other biometric live sample submitted by the applicant during the identity proofing event. The automated biometric comparison system uses a mathematical algorithm for the comparison. ● **Control of a digital account**. An individual is able to demonstrate control of a digital account (e.g., online bank account) or signed digital assertion (e.g., verifiable credentials) through the use of authentication or federation protocols. This may be done in person through presentation of the credential to a device or reader, but is more likely to be done during remote identity proofing sessions.	
5. Identity Assurance Level Requirements	
5.1. General Requirements	
5.1.1. Identity Service Documentation and Records	
The CSP **SHALL** conduct its operations according to a practice statement that details all identity proofing processes as they are implemented to achieve the defined IAL	
The practice statement **SHALL** include, at a minimum: 1. A complete service description including the particular steps the CSP follows to identity proof applicants at each offered assurance level; 2. Types of identity evidence the CSP accepts to meet the evidence strength requirements; 3. If applicable, alternative ways for an individual applicant who does not possess the required identity evidence to complete	IA-1 a. 2

Commented [6]: Several requirements in 800-63 are specified for CSPs or other entities. 800-53 does not have an equivalent concept. Should our mapping incorporate this difference somehow? If so, what is the best way?

the identity proofing process[1]; 4. The attributes the CSP considers to be core attributes. Core attributes include the minimum set of attributes the CSP needs to perform identity resolution as well as any additional attributes the CSP collects and validates for the purposes of identity proofing, fraud mitigation, complying with laws or legal process, or conveying to relying parties (RPs) through attribute assertions; 5. The CSP's policy and process for dealing with identity proofing errors; 6. The CSP's policy and process for identifying and communicating suspected or confirmed fraudulent accounts to RPs and affected individuals; 7. The CSP's policy for managing and communicating service changes (e.g., change in data sources, integrated vendors, or biometric algorithms) to RPs; 8. The CSP's policy for conducting privacy risk assessments, including the timing of its periodic reviews and specific conditions that will trigger an updated privacy risk assessment (see Section 5.1.2); 9. The CSP's policy for conducting assessments to determine potential equity impacts, including the timing of its periodic reviews and any specific conditions that will trigger an out-of-cycle review (see Section 5.1.3); and	
5.1.1.1. Ceasing Operations	
The CSP **SHALL** document its policy and plan for when it ceases its operations.	
This plan **SHALL** include whether the CSP's identity service is subject to retention requirements and how it will protect any sensitive data (including identity attributes, and information contained in subscriber accounts and audit logs) during the period of retention.	
At the end of any required retention period, the CSP **SHALL** be responsible for fully disposing of or destroying all sensitive data.	
5.1.1.2. Fraud Mitigation Measures	
The CSP **SHOULD** obtain additional confidence in identity proofing using fraud mitigation measures (e.g., examining the device	

characteristics of the applicant, evaluating behavioral characteristics, and checking vital statistic repositories such as the Death Master File ([DMF]).	
In the event the CSP uses fraud mitigation measures, the CSP **SHALL** conduct a privacy risk assessment for these mitigation measures.	
Such assessments **SHALL** include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per these guidelines.	
5.1.2. General Privacy Requirements	
5.1.2.1. Privacy Risk Assessment	
The CSP **SHALL** conduct and document a privacy risk assessment for the processes used for identity proofing and enrollment	
At a minimum, the privacy risk assessment **SHALL** assess the risks associated with: ● Any processing of PII for the purpose of identity proofing and enrollment, including identity attributes, biometrics, images, video, scans, or copies of identity evidence; ● Any additional steps the CSP takes to verify the identity of an applicant beyond the mandatory requirements specified herein; ● Any processing of PII for purposes outside the scope of identity proofing and enrollment except to comply with law or legal process; ● The retention schedule for identity records and PII; and, ● Any PII that is processed by a third party service on behalf of the CSP.	
Based on the results of its privacy risk assessment, the CSP **SHALL** document the measures it takes to maintain the disassociability, predictability, manageability, confidentiality, integrity, and availability of the PII it processes.	IA-8 (6)
In determining such measures, the CSP **SHALL** consult the *NIST Privacy Framework* [NIST-Privacy] and NIST Special Publication	IA-1 a. 1. (b)

[SP800-53].	
The CSP **SHALL** re-assess privacy risks and update its privacy risk assessment any time it makes changes to its identity service that affect the processing of PII	
The CSP **SHALL** review its privacy risk assessment periodically, as documented in its practice statement, to ensure it accurately reflects the current risks associated with the processing of PII.	
The CSP **SHALL** make a summary of its privacy risk assessment available to any organizations that use its services. The summary **SHALL** be in sufficient detail to enable such organizations to do due dilligence.	
5.1.2.2. Additional Privacy Protective Measures	
Processing of PII **SHALL** be limited to the minimum necessary to validate the existence of the claimed identity, associate the claimed identity with the applicant, and provide RPs with attributes they may use to make authorization decisions.	
The CSP **MAY** collect the Social Security Number (SSN) as an attribute when necessary for identity resolution, in accordance with the privacy requirements in Sec. 5.1.2.	IA-12 b.
Additionally, CSPs **SHALL** implement privacy protective techniques (e.g., transmitting and accepting derived attribute values rather than full attribute values themselves) to limit the proliferation and retention of SSN data. Knowledge of the SSN **SHALL NOT** be considered identity evidence.	
At the time of collection, the CSP **SHALL** provide explicit notice to the applicant regarding the purpose for collecting attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, the specific attributes and other sensitive data that the CSP intends to store in the applicant's subsequent subscriber account, the consequences for not providing the attributes, and the details of any records retention requirement if one is in place.	
The CSP **SHALL** provide mechanisms for redress of applicant	

complaints and for problems arising from the identity proofing. These mechanisms **SHALL** be easy for applicants to find and use. The CSP **SHALL** assess the mechanisms for their efficacy in achieving resolution of complaints or problems.	
5.1.3. General Equity Requirements	
In support of the goal of improved equity, and as part of its overall risk assessment process, the CSP **SHALL** assess the elements of its identity service to identify processes or technologies that can possibly result in inequitable access, treatment, or outcomes for members of one group as compared to others. See Sec. 10 for a non-exhaustive list of identity proofing processes and technologies that may be subject to inequitable access or outcomes.	
When assessing the risk of inequitable access, treatment, or outcomes, the following requirements apply: Based on the results of its risk assessment, the CSP **SHALL** document the measures it takes to mitigate the possibility of inequitable access, treatment, or outcomes.	
The CSP **SHALL** re-assess the risks to equitable access, treatment, or outcomes any time it makes changes to its identity service that affect the processes or technologies.	
The CSP **SHALL** re-assess the risks to equitable access, treatment, or outcomes periodically to ensure it accurately reflects the current risks associated with its service.	
The CSP **SHALL NOT** make applicant participation in these risk assessments mandatory.	
The CSP **SHALL** make the results of its assessment of risks associated with inequitable access, treatment, or outcomes, and any associated mitigations, available to any organizations or individuals that use its service.	
The CSP **SHALL** also make the results of its assessment publicly available.	

5.1.4. General Security Requirements	
Each online transaction within the identity proofing process, including transactions that involve third parties, **SHALL** occur over an authenticated protected channel.	
All PII, in the form of identity attributes, collected as part of the identity proofing process **SHALL** be protected to ensure the confidentiality and integrity of the information.	
The CSP **SHALL** assess the risks associated with operating its identity service, according to the NIST risk management framework [NIST-RMF], and apply an appropriate baseline security controls.	IA-1 a. 1. (b)
5.1.5. Additional Requirements for Federal Agencies	
The agency **SHALL** consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII, including biometrics, to conduct identity proofing triggers Privacy Act requirements.	
The agency **SHALL** consult with their SAOP to conduct an analysis determining whether the collection of PII, including biometrics, to conduct identity proofing triggers E-Government Act of 2002 [E-Gov] requirements.	IA-1 a. 1. (b)
The agency **SHALL** publish a System of Records Notice (SORN) to cover such collection, as applicable.	IA-1 a.1 (a)
The agency **SHALL** publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.	IA-1 a.1 (a)
The agency **SHALL** consult with the senior official, office, or governance body responsible for diversity, equity, inclusion, and accessibility (DEIA) for their agency to determine how the identity proofing service should be designed, resourced, and administered to meet the needs of all served populations.	IA-1 a.1 (a)
The agency **SHOULD** consult with public affairs and communications professionals within their organization to determine if a communications or public awareness strategy	

Commented [7]: Question for the group - does this apply to applications that don't do identity proofing, such as RPs? Should we distinguish in the mapping?

should be developed to accompany the roll-out of any new process, or an update to an existing process, including requirements associated with identity proofing. This may include materials detailing information about how to use the technology associated with the service, a Frequently Asked Questions (FAQs) page, prerequisites to participate in the identity proofing process (such as required evidence), webinars or other live or pre-recorded information sessions, or other media to support adoption and provide applicants with a mechanism to communicate questions, issues, and feedback.	
If the agency uses a third-party CSP, the agency **SHALL** be responsible for conducting its own privacy risk assessments or doing due diligence before relying on the CSP's privacy risk assessment as part of its PIA process.	IA-8 (2) (b)
If the agency uses a third-party CSP, the agency **SHALL** incorporate the CSP's assessment of equity risks into its own assessment of equity risks.	IA-8 (2) (b)
5.1.6. Requirements for Enrollment Codes	
Enrollment codes **SHALL** be sent to a validated address (e.g., postal address, telephone number, or email address).	IA-12 (5)
The applicant **SHALL** present a valid enrollment code to complete the identity proofing process.	
Enrollment codes **SHALL** be comprised of one of the following: A random six digit number generated by an approved random number generator with at least 20 bits of entropy; A secure link delivered to a uniquely identified address containing an appropriately constructed session ID (at least 64 bits of entropy); or A machine readable optical label (such as a QR code) that contains a random secret with at least 20 bits of entropy.	
Enrollment codes **SHALL** be valid for at most: 21 days, when sent to a validated postal address within the contiguous United States;	

30 days, when sent to a validated postal address outside the contiguous United States; 10 minutes, when sent to a validated telephone number (SMS or voice); or 24 hours, when sent to a validated email address.	
The enrollment code **SHALL NOT** be used as an authentication factor.	
5.1.7. Requirements for Notifications of Identity Proofing	
SHALL be sent to a validated address (e.g., postal address, telephone number, or email address) of record. Whenever possible, CSPs **SHOULD** send notifications of proofing and enrollment codes to different validated addresses.	IA-12 (5)
SHALL include details about the identity proofing event, such as the name of the identity service and the date the identity proofing was completed.	
SHALL provide clear instructions, including contact information, on actions to take in the case the recipient repudiates the identity proofing event.	
SHOULD provide additional information, such as how the organization or CSP protects the security and privacy of the information it collects and any responsibilities the recipient has as a subscriber of the identity service.	
5.1.8. Requirements for Use of Biometrics	
CSPs **SHALL** provide clear, publicly available information about all uses of biometrics, what biometric data is collected, how it is stored, and information on how to remove biometric information consistent with applicable laws and regulations.	
CSPs **SHALL** collect an explicit biometric consent from all applicants before collecting biometric information.	
CSPs **SHALL** store the biometric consent with the subscriber's	

account.	
CSPs **SHALL** have a documented, and publicly available, deletion process and default retention period for all biometric information.	
CSPs **SHALL** allow individuals to request deletion of their biometric information at any time, except where otherwise restricted by regulation, law, or statute.	
CSPs **SHALL** have all biometric algorithms tested by an independent entity (e.g., accredited laboratory or research institution) for performance, including performance across demographic groups.	
Testing of all algorithms **SHALL** be consistent with published ISO/IEC standards for the given modality.	IA-1 a. 1. (b)
CSPs **SHALL** meet the minimum performance thresholds for biometric usage: False match rate: 1:10,000 or better; and False non-match rate: 1:100 or better	
CSPs **SHALL** employ biometric technologies that provide similar performance characteristics for applicants of different demographic groups (racial background, gender, ethnicity, etc.). If performance differences across demographic groups are discovered, CSPs **SHALL** act expeditiously to provide redress options to affected individuals and to close performance gaps.	
CSPs **SHALL** make all performance and operational test results publicly available.	
CSPs **SHALL** assess the performance and demographic impacts of employed biometric technologies in conditions substantially similar to the operational environment and user base of the system. When such assessments include real-world users, participation by users **SHALL** be voluntary.	
CSPs **SHALL** make all performance and operational test results	

Commented [8]: CSP specific requirement

publicly available.	
CSP **SHALL** collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject.	
When collecting and comparing biometrics remotely, the CSP **SHALL** implement liveness detection capabilities to confirm the genuine presence of a live human being and to mitigate spoofing and impersonation attempts.	
When collecting biometrics in person, the CSP **SHALL** have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.	
5.1.9. Trusted Referees and Applicant References	
5.1.9.1. Requirements for Trusted Referees	
CSPs **SHALL** provide the option for the use of trusted referees for remote identity proofing at IALs 1 and 2.	
Where trusted referees are offered, the following requirements apply to their use: The CSP **SHALL** establish written policies and procedures for the use of trusted referees as part of its practice statement, as specified in Sec. 5.1.1.	
The CSP **SHALL** train its trusted referees to make risk-based decisions that allow applicants to be successfully identity proofed based on their unique circumstances.	
The CSP **SHALL** provide notification to the public of the availability of trusted referee services and how such services are obtained.	
5.1.9.2. Requirements for Applicant References	
CSPs **SHOULD** allow the use of applicant references.	
The following requirements apply to the use of applicant references	

at any IAL: The CSP **SHALL** establish written policies and procedures for the use of applicant references as part of its practice statement, as specified in Sec. 5.1.1.	
The CSP **SHALL** identity proof an applicant reference to the same or higher IAL intended for the applicant.	
If the CSP allows for the use of applicant references, it **SHALL** provide notification to the public of the allowability of applicant references and any requirements for the relationship between the reference and the applicant.	
5.1.10. Requirements for Interacting with Minors	
The CSP **SHALL** establish written policy and procedures as part of its practice statement for identity proofing minors who may not be able to meet the evidence requirements for a given IAL.	IA-1 a. 2
When interacting with persons under the age of 13, the CSP **SHALL** ensure compliance with the Children's Online Privacy Protection Act of 1998 [COPPA].	IA-1 a. 1. (b)
CSPs **SHALL** support the use of applicant references when interacting with individuals under the age or 18.	
5.2. Identity Proofing Process	
5.3. Identity Assurance Level 1	
5.3.1. Automated Attack Prevention	
The CSP **SHALL** implement a means to prevent automated attacks on the identity proofing process. Acceptable means include, but are not limited to: bot detection, mitigation, and management solutions; behavioral analytics; web application firewall settings; and traffic analysis.	

Commented [9]: CSP specific requirement

Commented [10]: CSP specific requirement

5.3.2. Evidence and Core Attributes Collection Requirements	
5.3.2.1. Evidence Collection	
For remote or in-person identity proofing, the CSP **SHALL** collect *one* of the following from the applicant: 1. One piece of SUPERIOR evidence, or 2. One piece of STRONG evidence and one piece of FAIR evidence	IA-12 a., IA-12 (2)
5.3.2.2. Collection of Additional Attributes	
Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes the CSP considers core attributes, it **MAY** collect attributes that are self-asserted by the applicant.	
5.3.3. Evidence and Core Attributes Validation Requirements	
The CSP **SHALL** validate the genuineness of each piece of SUPERIOR and STRONG evidence by *one* of the following: 1. Visual inspection by trained personnel 2. The use of technologies that can confirm the integrity of physical security features or detect if the evidence is fraudulent or has been inappropriately modified 3. If present, confirming the integrity of digital security features	IA-12 c.
The CSP **SHALL** validate the genuineness of each piece of FAIR evidence by visual inspection by trained personnel	IA-12 c.
The CSP **SHALL** validate all core attributes by *both*: 1. Validating the accuracy of attributes (such as account or reference number, name, and date of birth) obtained from pieces of evidence by comparison with authoritative or credible sources, and 2. Validating the accuracy of self-asserted attributes by comparison with authoritative or credible sources.	IA-12 c.
For added assurance, the CSP **SHALL** evaluate the core attributes,	

as validated by various sources, for overall consistency.	
5.3.4. Identity Verification Requirements	
The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the following: 1. Physical comparison of the applicant's face or biometric comparison of the facial image of the applicant to the facial portrait included on a piece of SUPERIOR or STRONG evidence, or 2. Demonstrated association with a digital account through an AAL1 authentication or an AAL1 and FAL1 federation protocol, or 3. Verification of the applicant's return of a valid enrollment code Sec. 5.1.6	IA-5 a., IA-8 (2) (a), IA-12 a.
5.3.5. Notification of Proofing Requirement	
Upon the successful completion of identity proofing at IAL1, the CSP **SHOULD** send a notification of proofing to a validated address for the applicant, as specified in Sec. 5.1.7.	
5.4. Identity Assurance Level 2	
5.4.1. Automated Attack Prevention	
The CSP **SHALL** implement a means to prevent automated attacks on the identity proofing process. Acceptable means include, but are not limited to: bot detection, mitigation, and management solutions; behavioral analytics; web application firewall settings; and traffic analysis.	
5.4.2. Evidence and Core Attribute Collection Requirements	
5.4.2.1. Evidence Collection	
For remote or in-person identity proofing, the CSP **SHALL** collect *one* of the following from the applicant: 1. One piece of SUPERIOR evidence 2. One piece of STRONG evidence and one piece of FAIR evidence	IA-12 c., IA-12 (2)

5.4.2.2. Collection of Attributes	
Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes the CSP considers core attributes, it **MAY** collect attributes that are self-asserted by the applicant.	IA-12 c.
5.4.3. Evidence and Core Attributes Validation Requirements	
The CSP **SHALL** validate the genuineness of each piece of SUPERIOR and STRONG evidence by one of the following: 1. Visual inspection by trained personnel 2. The use of technologies that can confirm the integrity of physical security features or detect if the evidence is fraudulent or has been inappropriately modified 3. If present, confirming the integrity of digital security features	IA-12 c.
The CSP **SHALL** validate all core attributes by: 1. Validating the accuracy of attributes (such as account or reference number, name, and date of birth) obtained from pieces of evidence by comparison with authoritative or credible sources, and 2. validating the accuracy of self-asserted attributes by comparison with authoritative or credible sources	IA-12 c.
For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various sources, for overall consistency.	
5.4.4. Identity Verification Requirements	
5.4.4.1. Remote Identity Proofing	
The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the following: 1. Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric contained on a piece of presented SUPERIOR or STRONG evidence 2. Demonstrated association with a digital account through an AAL2 authentication or an AAL2 and FAL2 federation	IA-5 a., IA-8 (2) (a), IA-12 a.

protocol	
5.4.4.2. In-person Identity Proofing	
The CSP **SHALL** verify the binding of the applicant to the claimed identity by physical or biometric comparison of the facial image of the applicant to the facial portrait contained on a piece of presented SUPERIOR or STRONG evidence.	IA-5 a., IA-12 a.
5.4.5. Notification of Proofing Requirement	
Upon the successful completion of identity proofing at IAL2, the CSP **SHALL** send a notification of proofing to a validated address for the applicant, as specified in Sec. 5.1.7.	
5.5. Identity Assurance Level 3	
5.5.1. Automated Attack Prevention	
The CSP **SHALL** implement a means to prevent automated attacks on the identity proofing process. Acceptable means include, but are not limited to: bot detection, mitigation, and management solutions; behavioral analytics; web application firewall settings; and traffic analysis.	
5.5.2. Evidence and Core Attributes Collection Requirements	
5.5.2.1. Evidence Collection	
The CSP **SHALL** collect evidence from the applicant according to *one* of the following options: 1. Two pieces of SUPERIOR evidence, or 2. One piece of SUPERIOR evidence and one piece of STRONG evidence, or 3. Two pieces of STRONG evidence and one piece of FAIR evidence	IA-12 c.
5.5.2.2. Collection of Attributes	
Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes the CSP considers core attributes, it **MAY** collect attributes that are	

self-asserted by the applicant.	
5.5.3. Validation Requirements	
5.5.3.1. Evidence Validation Requirements	
The CSP **SHALL** validate the genuineness of each piece of SUPERIOR evidence by confirming the integrity of its cryptographic security features and validating any digital signatures.	IA-12 c.
The CSP **SHALL** validate the genuineness of each piece of STRONG evidence by *one* of the following: 1. Visual inspection by trained personnel 2. The use of technologies that can confirm the integrity of physical security features and detect if the evidence is fraudulent or has been inappropriately modified 3. If present, confirming the integrity of digital security features, including the validity of the issuer's digital signature	IA-12 c.
5.5.3.2. Core Attribute Validation Requirements	
The CSP **SHALL** validate all core attributes by *both*: 1. Validating the accuracy of attributes obtained from pieces of evidence or applicant self-assertion by comparison with authoritative or credible sources 2. Validating the cryptographic features of any presented digital evidence, as described above	IA-12 c.
For added assurance, the CSP **SHALL** evaluate the core attributes, as validated by various sources, for overall consistency.	
5.5.4. Identity Verification Requirements	
The CSP **SHALL** verify the binding of the applicant to the claimed identity by *one* of the following: 1. Comparison of a collected biometric characteristic, such as a facial image, to the associated reference biometric characteristic contained on a piece of presented SUPERIOR or STRONG evidence 2. Demonstrated association with a digital account through, at	IA-5 a., IA-8 (2) (a), IA-12 a.

a minimum, an AAL2 authentication or an AAL2 and FAL2 federation protocol	
5.5.5 Notification of Proofing Requirement	
Upon the successful completion of identity proofing at IAL3, the CSP **SHALL** send a notification of proofing to a validated address for the applicant, as specified in Sec. 5.1.7.	
5.5.6. Biometric Collection	
The CSP **SHALL** collect and record a biometric sample at the time of proofing (e.g., facial image, fingerprints) for the purposes of non-repudiation and re-proofing.	
5.5.7. In-person Proofing Requirements	
In-person proofing at IAL3 **SHALL** be conducted in *one* of two ways: ● An in-person interaction between the applicant and a CSP operator, or ● A remote interaction with the applicant, supervised by an operator, based on the requirements in Sec. 5.5.8, *IAL3 Supervised Remote Identity Proofing*.	IA-5 a., IA-12 a., IA-12 (2), IA-12(4)* Note that supervised remote is also allowed.
Regardless of which of the two methods the CSP employs, the following requirements apply to identity proofing at IAL3: 1. The CSP **SHALL** have the operator view the biometric source (e.g., fingers, face) for the presence of any non-natural materials. 2. The CSP **SHALL** collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject.	
5.5.8. Requirements for IAL3 Supervised Remote Identity Proofing	
The following requirements apply to all IAL3 Supervised Remote Identity Proofing sessions: The CSP **SHALL** monitor the entire identity proofing session, and **SHALL** ensure the applicant is continuously present during the entire identity proofing session — for example, by a continuous	IA-12 a., IA-12 (2)

high-resolution video transmission of the applicant.	
The CSP **SHALL** have a live operator participate remotely with the applicant for the entirety of the identity proofing session.	IA-12 a., IA-12 (2)
The CSP **SHALL** require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.	IA-12 a., IA-12 (2)
The CSP **SHALL** require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors (e.g., embedded fingerprint reader).	IA-12 a., IA-12 (2), IA-12 (3)
The CSP **SHALL** require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.	IA-12 a., IA-12 (2)
The CSP **SHALL** employ physical tamper detection and resistance features appropriate for the environment in which it is located. For example, a kiosk located in a restricted area or one where it is monitored by a trusted individual requires less tamper detection than one that is located in a semi-public area such as a shopping mall concourse.	IA-12 a., IA-12 (2)
The CSP **SHALL** ensure that all communications occur over a mutually authenticated protected channel.	IA-12 a., IA-12 (2)
5.6. Summary of Requirements	
6. Subscriber Accounts	
6.1. Subscriber Accounts	
With the exception of identity proofing for the purposes of providing one-time access to an online service, or when an applicant declines enrollment into an account, the CSP **SHALL** enroll the applicant as a subscriber into its identity service and establish a unique *subscriber account* for that subscriber following the successful identity proofing of an applicant.	IA-2, IA-4 b., IA-4 c., IA-8

The CSP **SHALL** assign a unique identifier to each subscriber account.	IA-2, IA-4 b., IA-4 c., IA-8, IA-8(6)
At a minimum the CSP **SHALL** include the following information in each subscriber account: ● Unique identifier established for the subscriber ● A record of the identity proofing steps completed for the subscriber in accordance with Sec. 5.1.1 ● Maximum IAL successfully achieved for the identity proofing of the subscriber ● Subscriber consent provided for the processing, retention, or disclosure of any personal or sensitive information maintained in the subscriber account ● All authenticators currently bound to the subscriber account, whether registered at enrollment or subsequent to enrollment ● All attributes that were validated during the identity proofing process or in subsequent transactions to support RP access	IA-2, IA-4 b., IA-4 c., IA-4(9), IA-8
The CSP **SHALL** record information in the subscriber account that was collected during the identity proofing process or subsequently updated for each subscriber, including: ● Validated identity evidence ● Validated attribute information ● Attribute information that was collected for enrollment in the CSP identity service that was not validated for identity proofing purposes	IA-4(9)
The CSP **SHALL** perform a privacy risk assessment for the processing, retention, or disclosure of any personal information maintained in the subscriber account in accordance with Sec. 5.1.2.	
6.2. Subscriber Account Access	
In order to meet the requirement that accounts containing PII be protected by multi-factor authentication (MFA), the CSP **SHALL** provide a way for subscribers to access the information in their subscriber account through AAL2 or AAL3 authentication processes using authenticators registered to the subscriber account.	

The CSP **SHALL** provide the capability for subscribers to change or update the personal information contained in their subscriber account.	
6.3. Subscriber Account Lifecycle	
6.3.1. Subscriber Account Activity	
The CSP SHALL establish and maintain a unique subscriber account for each active subscriber in the CSP identity system from the time of enrollment to the time of account closure, as described below.	
Until the account is closed, the CSP SHALL provide for the use of the subscriber account, information contained in the account, and registered authenticators.	
6.3.2. Subscriber Account Termination	
The CSP **SHALL** terminate the subscriber account and discontinue its use when one of the following occur: ● The subscriber elects to terminate their subscriber account with the CSP. ● The CSP determines, following any due notice period and requirements established by the CSP, that the subscriber account has been compromised. ● The CSP determines, following any due notice period and requirements established by the CSP, that the subscriber has violated the policies or rules for participation in the CSP identity service. ● The CSP determines, following any due notice period and requirements established by the CSP, that the subscriber account is inactive in accordance with the policies or rules established by the CSP. ● The CSP ceases identity system and services operations.	
The CSP **SHALL** delete any personal or sensitive information from the subscriber account records following account termination in accordance with the record retention and disposal requirements.	

7. Threats and Security Considerations (Informative)	
7.1. Threat Mitigation Strategies (Informative)	
7.2. Collaboration with Adjacent Programs (Informative)	
8. Privacy Considerations (Informative)	
8.1. Collection and Data Minimization (Informative)	
8.1.1. Social Security Numbers (Informative)	
8.2. Notice and Consent (Informative)	
8.3. Use Limitation (Informative)	
8.4. Redress (Informative)	
8.5. Privacy Risk Assessment (Informative)	
8.6. Agency-Specific Privacy Compliance (Informative)	
9. Usability Considerations (Informative)	
9.1. General User Considerations During Enrollment and Identity Proofing (Informative)	
9.2. Pre-Enrollment Preparation (Informative)	
9.3. Enrollment and Proofing Session (Informative)	
9.4. Post-Enrollment (Informative)	
10. Equity Considerations (Informative)	
10.1. Equity and Identity Resolution (Informative)	
10.2. Equity and Identity Validation (Informative)	
10.3. Equity and Identity Verification (Informative)	
10.4. Equity and User Experience (Informative)	

800-63B-4

NIST 800-63B Reference	800-53 rev 5 control
1. Purpose (Informative)	
2. Introduction (Informative)	
3. Definitions and Abbreviations (Informative)	
4. Authentication Assurance Levels	
To satisfy the requirements of a given AAL and be recognized as a subscriber, a claimant **SHALL** be authenticated with a process whose strength is equal to or greater than the requirements at that level.	IA-8 (2) (a)
The result of an authentication process is an identifier that **SHALL** be used each time that subscriber authenticates to that RP.	IA-2, IA-8
The identifier **MAY** be pseudonymous.	IA-2, IA-8, IA-8 (6)
Subscriber identifiers **SHOULD NOT** be reused for a different subject but **SHOULD** be reused when a previously enrolled subject is re-enrolled by the CSP.	IA-2, IA-4 d., IA-8
Other attributes that identify the subscriber as a unique subject **MAY** also be provided.	IA-2, IA-8
Personal information collected during and subsequent to identity proofing **MAY** be made available to the subscriber by the digital identity service.	
The release or online availability of any PII or other personal information, whether self-asserted or validated, by federal government agencies requires multi-factor authentication in accordance with [EO13681]. Therefore, federal government agencies **SHALL** select a minimum of AAL2 when PII or other personal information is made available online.	IA-1 a. 1. (b)

Commented [11]: IA-1. a. 1 (b) stipulates that documented policy must be "consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;" This policy references "requirements of a given AAL" but not a specific law, etc. Should this requirement map to that 800-53 control?

4.1. Authentication Assurance Level 1	
4.1.1. Permitted Authenticator Types	
AAL1 authentication **SHALL** occur by the use of any of the following authenticator types, which are defined in Sec. 5:	IA-8 (2) (a)
4.1.2. Authenticator and Verifier Requirements	
Cryptographic authenticators used at AAL1 **SHALL** use approved cryptography.	
Software-based authenticators that operate within the context of an operating system **MAY**, where applicable, attempt to detect compromise (e.g., by malware) of the user endpoint in which they are running and **SHOULD NOT** complete the operation when such a compromise is detected.	IA-5 g, IA-5 h.
Communication between the claimant and verifier **SHALL** be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to adversary-in-the-middle (AitM) attacks.	IA-5 g, IA-9
Verifiers operated by or on behalf of federal government agencies at AAL1 **SHALL** be validated to meet the requirements of [FIPS140] Level 1.	IA-1 a.1 (b)
4.1.3. Reauthentication	
Periodic reauthentication of subscriber sessions **SHALL** be performed as described in Sec. 7.2.	IA-11
At AAL1, reauthentication of the subscriber **SHOULD** be repeated at least once per 30 days during an extended usage session, regardless of user activity.	IA-11
The session **SHOULD** be terminated (i.e., logged out) when this time limit is reached.	
4.1.4. Security Controls	
The CSP **SHALL** employ appropriately tailored security controls	IA-1 a.1 (b), IA-5 g, IA-5 (6)

Commented [12]: CSP specific requirement

from the baseline security controls defined in [SP800-53] or equivalent federal (e.g., [FEDRAMP]) or industry standard that the organization has determined for the information systems, applications, and online services that these guidelines are used to protect.	
The CSP **SHALL** ensure that the minimum assurance-related controls for the appropriate systems, or equivalent, are satisfied.	
4.1.5. Records Retention Policy	
The CSP **SHALL** comply with its respective records retention policies in accordance with applicable laws, regulations, and policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply.	IA-1 a.1 (b)
If the CSP opts to retain records in the absence of any mandatory requirements, the CSP **SHALL** conduct a risk management process, including assessments of privacy and security risks, to determine how long records should be retained and **SHALL** inform the subscriber of that retention policy.	
4.2. Authentication Assurance Level 2	
4.2.1. Permitted Authenticator Types	
At AAL2, authentication **SHALL** occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.	IA-8 (2) (a)
When a multi-factor authenticator is used, any of the following **MAY** be used: • Multi-Factor Out-of-Band Authenticator (Sec. 5.1.3.4) • Multi-Factor OTP Device (Sec. 5.1.5) • Multi-Factor Cryptographic Software (Sec. 5.1.8) • Multi-Factor Cryptographic Device (Sec. 5.1.9)	IA-2(6)(a) IA-8 (2) (a)
When a combination of two single-factor authenticators is used, the combination **SHALL** include a Memorized Secret authenticator (Sec. 5.1.1) and one physical authenticator (i.e., “something you have”)	IA-2(6)(a) IA-8 (2) (a)

Commented [13]: CSP specific requirement

from the following list: • Look-Up Secret (Sec. 5.1.2) • Out-of-Band Device (Sec. 5.1.3) • Single-Factor OTP Device (Sec. 5.1.4) • Single-Factor Cryptographic Software (Sec. 5.1.6) • Single-Factor Cryptographic Device (Sec. 5.1.7)	
4.2.2. Authenticator and Verifier Requirements	
Cryptographic authenticators used at AAL2 **SHALL** use approved cryptography.	
Authenticators procured by federal government agencies **SHALL** be validated to meet the requirements of [FIPS140] Level 1. Software-based authenticators that operate within the context of an operating system **MAY**, where applicable, attempt to detect compromise (e.g., by malware) of the platform in which they are running.	IA-1 a.1 (b) IA-5 g, IA-5 h.
They **SHOULD NOT** complete the operation when such a compromise is detected.	IA-5 g, IA-5 h.
At least one authenticator used at AAL2 **SHALL** be replay resistant as described in Sec. 5.2.8. Authentication at AAL2 **SHOULD** demonstrate authentication intent from at least one authenticator as discussed in Sec. 5.2.9.	IA-2(6)(b), IA2(8)
Communication between the claimant and verifier **SHALL** be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to AitM attacks.	IA-5 g
Verifiers operated by or on behalf of federal government agencies at AAL2 **SHALL** be validated to meet the requirements of [FIPS140] Level 1.	
When a biometric factor is used in authentication at AAL2, the performance requirements stated in Sec. 5.2.3 **SHALL** be met, and the verifier **SHOULD** make a determination that the biometric sensor and subsequent processing meet these requirements.	

While phishing resistance as described in Sec. 5.2.5 is not generally required for authentication at AAL2, verifiers **SHOULD** encourage the use of phishing-resistant authenticators at AAL2 whenever practical since phishing is a significant threat vector.	
4.2.3. Reauthentication	
Periodic reauthentication of subscriber sessions **SHALL** be performed as described in Sec. 7.2. At AAL2, authentication of the subscriber **SHALL** be repeated at least once per 12 hours during an extended usage session, regardless of user activity.	IA-11
Reauthentication of the subscriber **SHALL** be repeated following any period of inactivity lasting 30 minutes or longer.	IA-11
The session **SHALL** be terminated (i.e., logged out) when either of these time limits is reached.	
Reauthentication of a session that has not yet reached its time limit **MAY** require only a memorized secret or a biometric in conjunction with the still-valid session secret.	
The verifier **MAY** prompt the user to cause activity just before the inactivity timeout.	
4.2.4. Security Controls	
The CSP **SHALL** employ appropriately tailored security controls from the baseline security controls defined in [SP800-53] or equivalent federal (e.g., [FEDRAMP]) or industry standard that the organization has determined for the information systems, applications, and online services that these guidelines are used to protect.	IA-1 a.1 (b), IA-5 g, IA-5 (6)
The CSP **SHALL** ensure that the minimum assurance-related controls for the appropriate systems, or equivalent, are satisfied.	
4.2.5. Records Retention Policy	
The CSP **SHALL** comply with its respective records retention policies in accordance with applicable laws, regulations, and policies, including any NARA records retention schedules that may	IA-1 a.1 (b)

Commented [14]: CSP specific requirement

Commented [15]: CSP specific requirement

apply.	
If the CSP opts to retain records in the absence of any mandatory requirements, the CSP **SHALL** conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and **SHALL** inform the subscriber of that retention policy.	
4.3. Authentication Assurance Level 3	
AAL3 authentication **SHALL** use a hardware-based authenticator and an authenticator that provides phishing resistance — the same device **MAY** fulfill both these requirements.	IA-8 (2) (a)
In order to authenticate at AAL3, claimants **SHALL** prove possession and control of two distinct authentication factors through secure authentication protocols.	IA-8 (2) (a)
4.3.1. Permitted Authenticator Types	
AAL3 authentication **SHALL** occur by the use of one of a combination of authenticators satisfying the requirements in Sec. 4.3. Possible combinations are: ● Multi-Factor Cryptographic Device (Sec. 5.1.9) ● Single-Factor Cryptographic Device (Sec. 5.1.7) used in conjunction with a Memorized Secret (Sec. 5.1.1) ● Multi-Factor OTP device (software or hardware) (Sec. 5.1.5) used in conjunction with a Single-Factor Cryptographic Device (Sec. 5.1.7) ● Multi-Factor OTP device (hardware only) (Sec. 5.1.5) used in conjunction with a Single-Factor Cryptographic Software (Sec. 5.1.6) ● Single-Factor OTP device (hardware only) (Sec. 5.1.4) used in conjunction with a Multi-Factor Cryptographic Software Authenticator (Sec. 5.1.8)	IA-2(6)(a) IA-8 (2) (a)
4.3.2. Authenticator and Verifier Requirements	
Communication between the claimant and verifier **SHALL** be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to AitM attacks.	IA-5 g

At least one cryptographic authenticator used at AAL3 **SHALL** be phishing resistant as described in Sec. 5.2.5 and **SHALL** be replay resistant as described in Sec. 5.2.8.	IA-2(6)(b), IA2(8)
All authentication and reauthentication processes at AAL3 **SHALL** demonstrate authentication intent from at least one authenticator as described in Sec. 5.2.9.	
Multi-factor authenticators used at AAL3 **SHALL** be hardware cryptographic modules validated at [FIPS140] Level 2 or higher overall with at least [FIPS140] Level 3 physical security.	IA-1 a.1 (b), IA-2(6)(b)
Single-factor cryptographic devices used at AAL3 **SHALL** be validated at [FIPS140] Level 1 or higher overall with at least [FIPS140] Level 3 physical security.	IA-1 a.1 (b), IA-2(6)(b)
Verifiers at AAL3 **SHALL** be validated at [FIPS140] Level 1 or higher.	IA-1 a.1 (b)
Verifiers at AAL3 **SHALL** be verifier compromise resistant as described in Sec. 5.2.7 with respect to at least one authentication factor.	
Hardware-based authenticators and verifiers at AAL3 **SHOULD** resist relevant side-channel (e.g., timing and power-consumption analysis) attacks.	IA-2(6)(b)
When a biometric factor is used in authentication at AAL3, the verifier **SHALL** make a determination that the biometric sensor and subsequent processing meet the performance requirements stated in Sec. 5.2.3.	
4.3.3. Reauthentication	
Periodic reauthentication of subscriber sessions **SHALL** be performed as described in Sec. 7.2.	IA-11
At AAL3, authentication of the subscriber **SHALL** be repeated at least once per 12 hours during an extended usage session, regardless of user activity, as described in Sec. 7.2.	IA-11

Reauthentication of the subscriber **SHALL** be repeated following any period of inactivity lasting 15 minutes or longer.	IA-11
Reauthentication **SHALL** use both authentication factors.	
The session **SHALL** be terminated (i.e., logged out) when either of these time limits is reached.	
The verifier **MAY** prompt the user to cause activity just before the inactivity timeout.	
4.3.4. Security Controls	
The CSP **SHALL** employ appropriately tailored security controls from the baseline security controls defined in [SP800-53] or equivalent federal (e.g., [FEDRAMP]) or industry standard that the organization has determined for the information systems, applications, and online services that these guidelines are used to protect.	IA-1 a.1 (b), IA-5 g, IA-5 (6)
The CSP **SHALL** ensure that the minimum assurance-related controls for the appropriate systems, or equivalent, are satisfied.	
4.3.5. Records Retention Policy	
The CSP **SHALL** comply with its respective records retention policies in accordance with applicable laws, regulations, and policies, including any NARA records retention schedules that may apply.	IA-1 a.1 (b)
If the CSP opts to retain records in the absence of any mandatory requirements, the CSP **SHALL** conduct a risk management process, including assessments of privacy and security risks, to determine how long records should be retained and **SHALL** inform the subscriber of that retention policy.	
4.4. Privacy Requirements	
The CSP **SHALL** employ appropriately tailored privacy controls defined in [SP800-53] or equivalent industry standard.	IA-1 a.1 (b)
If CSPs process attributes for purposes other than identity	

Commented [16]: CSP specific requirement

Commented [17]: CSP specific requirement

Commented [18]: CSP specific requirement

proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, CSPs **SHALL** implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing	
Measures **MAY** include providing clear notice, obtaining subscriber consent, or enabling selective use or disclosure of attributes. When CSPs use consent measures, CSPs **SHALL NOT** make consent for the additional processing a condition of the identity service.	
Regardless of whether the CSP is an agency or private sector provider, the following requirements apply to a federal agency offering or using the authentication service: 1. The agency **SHALL** consult with their Senior Agency Official for Privacy (SAOP) and conduct an analysis to determine whether the collection of PII to issue or maintain authenticators triggers the requirements of the *Privacy Act of 1974* [PrivacyAct] (see Sec. 9.4).	IA-1 a.1 (b)
2. The agency **SHALL** publish a System of Records Notice (SORN) to cover such collections, as applicable.	
3. The agency **SHALL** consult with their SAOP and conduct an analysis to determine whether the collection of PII to issue or maintain authenticators triggers the requirements of the *E-Government Act of 2002* [E-Gov].	IA-1 a.1 (b)
4. The agency **SHALL** publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable	

4.5. Summary of Requirements	
5. Authenticator and Verifier Requirements	
5.1. Requirements by Authenticator Type	
5.1.1. Memorized Secrets	
5.1.1.1. Memorized Secret Authenticators	
Memorized secrets **SHALL** be at least 8 characters in length.	IA-5 (1) (h)
Memorized secrets **SHALL** be either chosen by the subscriber or assigned randomly by the CSP.	
If the CSP disallows a chosen memorized secret because it is on a blocklist of commonly used, expected, or compromised values (see Sec. 5.1.1.2), the subscriber **SHALL** be required to choose a different memorized secret.	IA-5 (1) (a)
No other complexity requirements for memorized secrets **SHALL** be imposed.	IA-5 (1) (h)
5.1.1.2. Memorized Secret Verifiers	
Verifiers **SHALL** require memorized secrets to be at least 8 characters in length.	IA-5 (1) (h), IA-5 (18)
Verifiers **SHOULD** permit memorized secrets to be at least 64 characters in length.	IA-5 (1) (h), IA-5 (18)
All printing ASCII [RFC20] characters as well as the space character **SHOULD** be acceptable in memorized secrets.	IA-5 (1) (h), IA-5 (1) (f)
Unicode [ISO/ISC 10646] characters **SHOULD** be accepted as well.	IA-5 (1) (h),
Verifiers **MAY** make allowances for likely mistyping, such as removing leading and trailing whitespace characters prior to verification or allowing verification of memorized secrets with differing case for the leading character, provided memorized secrets remain at least 8 characters in length after such	

Commented [19]: This 800-53 requirements contradicts the 800-63 requirement it references.

processing.	
Verifiers **SHALL** verify the entire submitted memorized secret (i.e., not truncate the secret). For purposes of the above length requirements, each Unicode code point **SHALL** be counted as a single character.	
If Unicode characters are accepted in memorized secrets, the verifier **SHOULD** apply the normalization process for stabilized strings using either the NFKC or NFKD normalization defined in Sec. 12.1 of *Unicode Normalization Forms* [UAX15].	IA-5 (1) (f)
Subscribers choosing memorized secrets containing Unicode characters **SHOULD** be advised that some characters may be represented differently by some endpoints, which can affect their ability to authenticate successfully.	IA-5 (1) (f)
Memorized secret verifiers **SHALL NOT** permit the subscriber to store a hint that is accessible to an unauthenticated claimant.	IA-5 (18)
Verifiers **SHALL NOT** prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?", a technique known as knowledge-based authentication (KBA) or security questions) when choosing memorized secrets.	
When processing requests to establish and change memorized secrets, verifiers **SHALL** compare the prospective secrets against a blocklist that contains values known to be commonly used, expected, or compromised.	IA-5 (1) (a), IA-5 (1) (h), IA-5 (18)
For example, the list **MAY** include, but is not limited to: ● Passwords obtained from previous breach corpuses. ● Dictionary words. ● Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd'). ● Context-specific words, such as the name of the service, the username, and derivatives thereof.	IA-5 (1) (a), IA-5 (1) (h), IA-5 (18)
If the chosen secret is found in the blocklist, the CSP or verifier **SHALL** advise the subscriber that they need to select a different secret, **SHALL** provide the reason for rejection, and **SHALL** require	IA-5 (1) (a), IA-5 (1) (b) IA-5 (18)

the subscriber to choose a different value.	
Since the blocklist is used to defend against brute-force attacks and unsuccessful attempts are rate limited as described below, the blocklist **SHOULD** be of a size sufficient to prevent subscribers from choosing memorized secrets that attackers are likely to guess before reaching the attempt limit.	IA-5 (1) (a) IA-5 (18)
Excessively large blocklists **SHOULD NOT** be used because they frustrate subscribers' attempts to establish an acceptable memorized secret and do not provide significantly improved security.	IA-5 (1) (a)
Verifiers **SHALL** offer guidance to the subscriber to assist the user in choosing a strong memorized secret. This is particularly important following the rejection of a memorized secret on the above list as it discourages trivial modification of listed (and likely very weak) memorized secrets [Blocklists].	IA-5 (1) (g)
Verifiers **SHALL** implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber account as described in Sec. 5.2.2.	IA-5 (18)
Verifiers **SHALL NOT** impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets	IA-5 (1) (h), IA-5 (18)
Verifiers **SHALL NOT** require users to periodically change memorized secrets.	IA-5 (18)
However, verifiers **SHALL** force a change if there is evidence of compromise of the authenticator.	IA-5 (18)
Verifiers **SHALL** allow the use of password managers.	IA-5 (18)
To facilitate their use, verifiers **SHOULD** permit claimants to use "paste" functionality when entering a memorized secret. Password manangers may increase the likelihood that users will choose stronger memorized secrets.	IA-5 (18)
In order to assist the claimant in successfully entering a memorized	IA-5 (18)

secret, the verifier **SHOULD** offer an option to display the secret — rather than a series of dots or asterisks — while it is entered and until it is submitted to the verifier.	IA-6
This allows the claimant to confirm their entry if they are in a location where their screen is unlikely to be observed. The verifier **MAY** also permit the claimant's device to display individual entered characters for a short time after each character is typed to verify correct entry. This is common on mobile devices.	IA-5 (18)
The verifier **SHALL** use approved encryption and an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and adversary-in-the-middle attacks.	IA-5 g, IA-5 (1) (c)
Verifiers **SHALL** store memorized secrets in a form that is resistant to offline attacks	IA-5 (18)
Memorized secrets **SHALL** be salted and hashed using a suitable password hashing scheme. Password hashing schemes take a password, a salt, and a cost factor as inputs and generate a password hash.	IA-5 g, IA-5 (1) (d) IA-5 (18)
A function that is both memory-hard and compute-hard **SHOULD** be used because it increases the cost of an attack.	IA-5 g, IA-5 (1) (d) IA-5 (18)
The chosen output length of the password hashing scheme **SHOULD** be the same as the length of the underlying one-way function output.	IA-5 g, IA-5 (1) (d) IA-5 (18)
The salt **SHALL** be at least 32 bits in length and be chosen arbitrarily so as to minimize salt value collisions among stored hashes.	IA-5 g, IA-5 (1) (d) IA-5 (18)
Both the salt value and the resulting hash **SHALL** be stored for each memorized secret authenticator.	IA-5 (18)
For the Password-based Key Derivation Function 2 (PBKDF2) [SP800-132], the cost factor is an iteration count: the more times the PBKDF2 function is iterated, the longer it takes to compute the password hash. Therefore, the iteration count **SHOULD** be as large	IA-5 (18)

as verification server performance will allow, typically at least 10,000 iterations.	
In addition, verifiers **SHOULD** perform an additional iteration of a keyed hashing or encryption operation using a secret key known only to the verifier.	IA-5 g, IA-5 (1) (d) IA-5 (18)
This key value, if used, **SHALL** be generated by an approved random bit generator [SP800-90Ar1] and provide at least the minimum security strength specified in the latest revision of NIST SP 800-131A, *Transitioning the Use of Cryptographic Algorithms and Key Lengths* [SP800-131A] (112 bits as of the date of this publication).	IA-1 a.1 (b), IA-5 (1) (d) IA-5 (18)
The secret key value **SHALL** be stored separately from the hashed memorized secrets (e.g., in a specialized device like a hardware security module).	IA-5 g, IA-5 (1) (d) IA-5 (18)
5.1.2. Look-Up Secrets	
5.1.2.1. Look-Up Secret Authenticators	
CSPs creating look-up secret authenticators **SHALL** use an approved random bit generator [SP800-90Ar1] to generate the list of secrets and **SHALL** deliver the authenticator securely to the subscriber. Look-up secrets **SHALL** have at least 20 bits of entropy	IA-1 a.1 (b) IA-5 g
Look-up secrets **MAY** be distributed by the CSP in person, by postal mail to the subscriber's address of record, or by online distribution. If distributed online, look-up secrets **SHALL** be distributed over a secure channel in accordance with the post-enrollment binding requirements in Sec. 6.1.2.	
If the authenticator uses look-up secrets sequentially from a list, the subscriber **MAY** dispose of used secrets, but only after a successful authentication	
5.1.2.2. Look-Up Secret Verifiers	
Verifiers of look-up secrets **SHALL** prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.	

Commented [20]: CSP specific requirement

A given secret from an authenticator **SHALL** be used successfully only once. If the look-up secret is derived from a grid card, each cell of the grid **SHALL** be used only once.	
Verifiers **SHALL** store look-up secrets in a form that is resistant to offline attacks.	
Look-up secrets having at least 112 bits of entropy **SHALL** be hashed with an approved one-way function as described in Sec. 5.1.1.2.	
Look-up secrets with fewer than 112 bits of entropy **SHALL** be salted and hashed using a suitable password hashing scheme, also described in Sec. 5.1.1.2.	
The salt value **SHALL** be at least 32 bits in length and arbitrarily chosen so as to minimize salt value collisions among stored hashes. Both the salt value and the resulting hash **SHALL** be stored for each look-up secret.	
For look-up secrets that have less than 64 bits of entropy, the verifier **SHALL** implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber account as described in Sec. 5.2.2.	
The verifier **SHALL** use approved encryption and an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and AitM attacks.	IA-5 g
5.1.3. Out-of-Band Devices	
5.1.3.1. Out-of-Band Authenticators	
The out-of-band authenticator **SHALL** establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request. This channel is considered to be out-of-band with respect to the primary communication channel (even if it terminates on the same device) provided the device does not leak information from one channel to the other without the authorization of the claimant.	IA-2(13) IA-5 g, IA-5 h.
The out-of-band device **SHOULD** be uniquely addressable by the	IA-2(13)

Commented [21]: Depending on other decisions, some Out Of Band are not phishing resistant, so they would not be approved.

verifier.	
Communication over the secondary channel **SHALL** be encrypted unless sent via the public switched telephone network (PSTN).	IA-2(13) IA-5 g
For additional authenticator requirements specific to use of the PSTN for out-of-band authentication, see Sec. 5.1.3.3. Channels or addresses that do not prove possession of a specific device, such as voice-over-IP (VOIP) telephone numbers, **SHALL NOT** be used for out-of-band authentication	IA-2(13) IA-5 g
Email **SHALL NOT** be used for out-of-band authentication because it also does not prove possession of a specific device and is typically accessed using only a memorized secret.	IA-2(13) IA-5 g
The out-of-band authenticator **SHALL** uniquely authenticate itself in one of the following ways when communicating with the verifier:	IA-2(13)
• Establish an authenticated protected channel to the verifier using approved cryptography. The key used **SHALL** be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).	IA-2(13)
• Authenticate to a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device. This method **SHALL** only be used if a secret is being sent from the verifier to the out-of-band device via the PSTN (SMS or voice).	IA-2(13)
If a secret is sent by the verifier to the out-of-band device, the device **SHOULD NOT** display the authentication secret while it is locked by the owner (i.e., **SHOULD** require the presentation and verification of a PIN, passcode, or biometric characteristic to view). However, authenticators **SHOULD** indicate the receipt of an authentication secret on a locked device.	IA-2(13) IA-5 g, IA-5 h.
If the out-of-band authenticator requests approval over the secondary communication channel — rather than by the presenting a secret that the claimant transfers to the primary communication channel — it **SHALL** accept transfer of the secret from the primary channel and send it to the verifier over the secondary channel to	IA-2(13)

associate the approval with the authentication transaction.	
The claimant **MAY** perform the transfer manually or use a technology such as a barcode or QR code to effect the transfer.	IA-2(13)
5.1.3.2. Out-of-Band Verifiers	
When the out-of-band authenticator is a secure application, such as on a smart phone, the verifier **MAY** send a push notification to that device.	IA-2(13)
The verifier waits for the establishment of an authenticated protected channel with the out-of-band authenticator and verifies its identifying key. The verifier **SHALL NOT** store the identifying key itself, but **SHALL** use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator. Once authenticated, the verifier transmits the authentication secret to the authenticator.	IA-2(13)
Depending on the type of out-of-band authenticator, one of the following **SHALL** take place:	IA-2(13)
• Transfer of secret from the secondary to the primary channel: The verifier **MAY** signal the device containing the subscriber's authenticator to indicate readiness to authenticate. It **SHALL** then transmit a random secret to the out-of-band authenticator. The verifier **SHALL** then wait for the secret to be returned on the primary communication channel.	IA-2(13)
• Transfer of secret from the primary to the secondary channel: The verifier **SHALL** display a random authentication secret to the claimant via the primary channel. It **SHALL** then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator.	IA-2(13)
In all cases, the authentication **SHALL** be considered invalid if not completed within 10 minutes.	IA-2(13)

In order to provide replay resistance as described in Sec. 5.2.8, verifiers **SHALL** accept a given authentication secret only once during the validity period.	IA2(8), IA-2(13)
The verifier **SHALL** generate random authentication secrets with at least 20 bits of entropy using an approved random bit generator [SP800-90Ar1].	IA-1 a.1 (b), IA-2(13)
If the authentication secret has less than 64 bits of entropy, the verifier **SHALL** implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber account as described in Sec. 5.2.2.	IA-2(13)
Out-of-band verifiers **SHALL** consider all authentication operations to be single-factor unless the CSP has confirmed that the out-of-band authentication meets the requirements of Sec. 5.1.3.4.	IA-2(13)
This requirement **MAY** be satisfied by issuance of the authenticator by the CSP or a trusted third party or by use of an authentication application known by the CSP to meet these requirements.	IA-2(13)
Out-of-band verifiers that send a push notification to a subscriber device **SHOULD** implement a reasonable limit on the rate or total number of push notifications that will be sent since the last successful authentication	IA-2(13)
5.1.3.3. Authentication using the Public Switched Telephone Network	
Use of the PSTN for out-of-band verification is restricted as described in this section and in Sec. 5.2.10. If out-of-band verification is to be made using the PSTN, the verifier **SHALL** verify that the pre-registered telephone number being used is associated with a specific physical device.	IA-2(13) IA-5 g
Changing the pre-registered telephone number is considered to be the binding of a new authenticator and **SHALL** only occur as described in Sec. 6.1.2.	
Use of the PSTN to deliver out-of-band authentication secrets is potentially not available to some subscribers in areas with limited telephone coverage (particularly in areas without mobile phone	IA-2(13)

Commented [22]: PSTN has been deprecated for government use.

service). Accordingly, verifiers **SHALL** ensure that alternative authenticator types are available to all subscribers and **SHOULD** remind subscribers of this limitation of PSTN out-of-band authenticators prior to binding.	
Verifiers **SHOULD** consider risk indicators such as device swap, SIM change, number porting, or other abnormal behavior before using the PSTN to deliver an out-of-band authentication secret.	IA-2(13)
5.1.3.4. Multi-Factor Out-of-Band Authenticators	
Each use of the authenticator **SHALL** require the presentation of the activation factor.	IA-2(13)
The use of an activation secret by the authenticator **SHALL** meet the requirements of Sec. 5.2.11	IA-2(13)
. A biometric activation factor **SHALL** meet the requirements of Sec. 5.2.3, including limits on the number of consecutive authentication failures.	IA-2(13)
Submission of the activation factor **SHALL** be a separate operation from unlocking of the host device (e.g., smartphone), although the same activation factor used to unlock the host device **MAY** be used in the authentication operation.	IA-2(13)
The memorized secret or biometric sample used for activation — and any biometric data derived from the biometric sample such as a probe produced through signal processing — **SHALL** be zeroized immediately after the authentication operation.	IA-2(13) IA-5 g,IA-5 h.
5.1.4. Single-Factor OTP Device	
5.1.4.1. Single-Factor OTP Authenticators	
The secret key and its algorithm **SHALL** provide at least the minimum security strength specified in the latest revision of [SP800-131A] (112 bits as of the date of this publication).	IA-1 a.1 (b)
The nonce **SHALL** be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.	

Commented [23]: Single-factor OTP has been deprecated as non-phishing resistant.

If a subscriber needs to change the device used for a software-based OTP authenticator, they **SHOULD** bind the authenticator application on the new device to their subscriber account as described in Sec. 6.1.2.1 and invalidate the authenticator application that will no longer be used.	
The authenticator output is obtained by using an approved block cipher or hash function to combine the key and nonce in a secure manner. The authenticator output **MAY** be truncated to as few as 6 decimal digits (approximately 20 bits of entropy).	
If the nonce used to generate the authenticator output is based on a real-time clock, the nonce **SHALL** be changed at least once every 2 minutes	
5.1.4.2. Single-Factor OTP Verifiers	
Single-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator. As such, the symmetric keys used by authenticators are also present in the verifier, and **SHALL** be strongly protected against unauthorized disclosure by the use of access controls that limit access to the keys to only those software components on the device requiring access.	
When a single-factor OTP authenticator is being associated with a subscriber account, the verifier or associated CSP **SHALL** use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.	
The verifier **SHALL** use approved encryption and an authenticated protected channel when collecting the OTP in order to provide resistance to eavesdropping and AitM attacks	IA-5 g
In order to provide replay resistance as described in Sec. 5.2.8, verifiers **SHALL** accept a given OTP only once while it is valid.	IA2(8)
In the event a claimant's authentication is denied due to duplicate use of an OTP, verifiers **MAY** warn the claimant in case an attacker has been able to authenticate in advance.	
Verifiers **MAY** also warn a subscriber in an existing session of the	

Commented [24]: OTP is not phishing resistant

attempted duplicate use of an OTP.	
Time-based OTPs [TOTP] **SHALL** have a defined lifetime that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.	
If the authenticator output has less than 64 bits of entropy, the verifier **SHALL** implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber account as described in Sec. 5.2.2.	
5.1.5. Multi-Factor OTP Devices	
The multi-factor OTP device is *something you have*, and it **SHALL** be activated by either *something you know* or *something you are*.	
5.1.5.1. Multi-Factor OTP Authenticators	
Multi-factor OTP authenticators operate in a similar manner to single-factor OTP authenticators (see Sec. 5.1.4.1), except that they require the presentation and verification of either a memorized secret or a biometric characteristic to obtain the OTP from the authenticator. Each use of the authenticator **SHALL** require the input of the activation factor.	
The secret key and its algorithm **SHALL** provide at least the minimum security strength specified in the latest revision of [SP800-131A] (112 bits as of the date of this publication).	IA-1 a.1 (b)
The nonce **SHALL** be of sufficient length to ensure that it is unique for each operation of the device over its lifetime	
If a subscriber needs to change the device used for a software-based OTP authenticator, they **SHOULD** bind the authenticator application on the new device to their subscriber account as described in Sec. 6.1.2.1 and invalidate the authenticator application that will no longer be used.	

Commented [25]: If OTP are not phishing resistant, and in light of OMB 22-09, should we not direct agencies to sections that are not compliant based on other Executive Memos?

The authenticator output is obtained by using an approved block cipher or hash function to combine the key and nonce in a secure manner. The authenticator output **MAY** be truncated to as few as 6 decimal digits (approximately 20 bits of entropy).	
If the nonce used to generate the authenticator output is based on a real-time clock, the nonce **SHALL** be changed at least once every 2 minutes.	
The use of an activation secret by the authenticator **SHALL** meet the requirements of Sec. 5.2.11.	
A biometric activation factor **SHALL** meet the requirements of Sec. 5.2.3, including limits on the number of consecutive authentication failures.	
Submission of the activation factor **SHALL** be a separate operation from unlocking of the host device (e.g., smartphone), although the same activation factor used to unlock the host device **MAY** be used in the authentication operation.	
The unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — **SHALL** be zeroized immediately after an OTP has been generated	IA-5 g,IA-5 h.
5.1.5.2. Multi-Factor OTP Verifiers	
Multi-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator, but without the requirement that a second factor be provided. As such, the symmetric keys used by authenticators **SHALL** be strongly protected against unauthorized disclosure by the use of access controls that limit access to the keys to only those software components on the device requiring access.	
When a multi-factor OTP authenticator is being associated with a subscriber account, the verifier or associated CSP **SHALL** use approved cryptography to either generate and exchange or to obtain the secrets required to duplicate the authenticator output.	
The verifier or CSP **SHALL** also establish, by issuance of the	

authentictor, that the authenticator is a multi-factor device. Otherwise, the verifier **SHALL** treat the authenticator as single-factor, in accordance with Sec. 5.1.4.	
The verifier **SHALL** use approved encryption and an authenticated protected channel when collecting the OTP in order to provide resistance to eavesdropping and AitM attacks.	IA-5 g
In order to provide replay resistance as described in Sec. 5.2.8, verifiers **SHALL** accept a given OTP only once while it is valid.	IA2(8)
In the event a claimant's authentication is denied due to duplicate use of an OTP, verifiers **MAY** warn the claimant in case an attacker has been able to authenticate in advance.	
Verifiers **MAY** also warn a subscriber in an existing session of the attempted duplicate use of an OTP.	
Time-based OTPs [TOTP] **SHALL** have a defined lifetime that is determined by the expected clock drift — in either direction — of the authenticator over its lifetime, plus allowance for network delay and user entry of the OTP.	
If the authenticator output or activation secret has less than 64 bits of entropy, the verifier **SHALL** implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber account as described in Sec. 5.2.2.	
5.1.6. Single-Factor Cryptographic Software	No requirements in section
5.1.6.1. Single-Factor Cryptographic Software Authenticators	
Single-factor cryptographic software authenticators encapsulate one or more secret keys unique to the authenticator. The key **SHALL** be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, or TEE if available).	IA-5 g, IA-5 h. IA-5 (2) (a) (1)
The key **SHALL** be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key	IA-5 (2) (a) (1)

Commented [26]: Non-Phishing Resistant

to only those software components on the device requiring access	
External cryptographic authenticators that do not meet the requirements of cryptographic hardware authenticators (e.g., that have a mechanism to allow private keys to be exported) are also considered to be cryptographic software authenticators. They **SHALL** meet the requirements for connected authenticators in Sec. 5.2.12.	
5.1.6.2. Single-Factor Cryptographic Software Verifiers	
5.1.7. Single-Factor Cryptographic Devices	
5.1.7.1. Single-Factor Cryptographic Device Authenticators	
Single-factor cryptographic device authenticators use tamper-resistant hardware to encapsulate one or more secret keys unique to the authenticator that **SHALL NOT** be exportable (i.e., cannot be removed from the device). The authenticator operates using a secret key to sign a challenge nonce presented through a direct interface between the authenticator and endpoint (e.g., a USB port or secured wireless connection) as specified in Sec. 5.2.12.	IA-5 g,IA-5 h.
The secret key and its algorithm **SHALL** provide at least the minimum security length specified in the latest revision of [SP800-131A] (112 bits as of the date of this publication). The challenge nonce **SHALL** be at least 64 bits in length. Approved cryptography **SHALL** be used.	IA-1 a.1 (b)
In order to be considered a cryptographic device, an authenticator **SHALL** either be a separate piece of hardware or an embedded processor or execution environment, e.g., secure element, trusted execution environment (TEE), trusted platform module (TPM).	IA-5 g, IA-5 h. IA-5 (2) (a) (1)
These hardware authenticators or embedded processors are separate from a host processor such as the CPU on a laptop or mobile device. A cryptographic device authenticator **SHALL** be designed so as to prohibit the export of the authentication secret to the host processor and **SHALL NOT** be capable of being reprogrammed by the host processor so as to allow the secret to be extracted. The authenticator is subject to applicable [FIPS140]	IA-1 a.1 (b), IA-5 g, IA-5 h. IA-5 (2) (a) (1) IA-7

requirements of the AAL at which the authenticator is being used.	
Single-factor cryptographic device authenticators **SHOULD** require a physical input (e.g., the pressing of a button) in order to operate.	IA-5 g,IA-5 h.
5.1.7.2. Single-Factor Cryptographic Device Verifiers	
The verifier has either symmetric or asymmetric cryptographic keys corresponding to each authenticator. While both types of keys **SHALL** be protected against modification, symmetric keys **SHALL** additionally be protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.	IA-5 g
The challenge nonce **SHALL** be at least 64 bits in length, and **SHALL** either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator [SP800-90Ar1]).	
The verification operation **SHALL** use approved cryptography	
5.1.8. Multi-Factor Cryptographic Software	
The multi-factor cryptographic software authenticator is *something you have*, and it **SHALL** be activated by either *something you know* or *something you are*.	IA-7
5.1.8.1. Multi-Factor Cryptographic Software Authenticators	
The key **SHOULD** be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE).	IA-5 g, IA-5 h.
The key **SHALL** be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.	IA-5 g, IA-5 h. IA-5 (2) (a) (1)
External cryptographic authenticators that do not meet the requirements of cryptographic hardware authenticators (e.g., that have a mechanism to allow private keys to be exported) are also considered to be cryptographic software authenticators. They **SHALL** meet the requirements for connected authenticators in Sec.	

5.2.12.	
Each authentication operation using the authenticator **SHALL** require the input of the activation factor.	IA-5 (2) (a) (1)
The use of an activation secret by the authenticator **SHALL** meet the requirements of Sec. 5.2.11.	IA-5 (2) (a) (1)
A biometric activation factor **SHALL** meet the requirements of Sec. 5.2.3, including limits on the number of consecutive authentication failures.	IA-5 (2) (a) (1)
Submission of the activation factor **SHALL** be a separate operation from unlocking of the host device (e.g., smartphone), although the same activation factor used to unlock the host device **MAY** be used in the authentication operation.	IA-5 (2) (a) (1)
The activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — **SHALL** be zeroized immediately after an authentication transaction has taken place	IA-5 g, IA-5 h. IA-5 (2) (a) (1)
5.1.8.2. Multi-Factor Cryptographic Software Verifiers	
5.1.9. Multi-Factor Cryptographic Devices	
The multi-factor cryptographic device is *something you have*, and it **SHALL** be activated by either *something you know* or *something you are*.	IA-7
5.1.9.1. Multi-Factor Cryptographic Device Authenticators	
Multi-factor cryptographic device authenticators use tamper-resistant hardware to encapsulate one or more secret keys unique to the authenticator that **SHALL NOT** be exportable (i.e., cannot be removed from the device).	IA-5 g, IA-5 h. IA-5 (2) (a) (1)
The secret key **SHALL** be accessible only through the presentation and verification of an activation factor, either a biometric characteristic or an activation secret as described in Sec. 5.2.11.	IA-5 (2) (a) (1)
The secret key and its algorithm **SHALL** provide at least the	IA-1 a.1 (b)

minimum security length specified in the latest revision of [SP800-131A] (112 bits as of the date of this publication).	
The challenge nonce **SHALL** be at least 64 bits in length. Approved cryptography **SHALL** be used.	
In order to be considered a cryptographic device, an authenticator **SHALL** either be a separate piece of hardware or an embedded processor or execution environment, e.g., secure element, trusted execution environment (TEE), trusted platform module (TPM).	IA-2(6)(a) IA-5 g, IA-5 h. IA-5 (2) (a) (1)
A cryptographic device authenticator **SHALL** be designed so as to prohibit the export of the authentication secret to the host processor and **SHALL NOT** be capable of being reprogrammed by the host processor so as to allow the secret to be extracted. The authenticator is subject to applicable [FIPS140] requirements of the AAL at which the authenticator is being used.	IA-1 a.1 (b) IA-5 g, IA-5 h. IA-5 (2) (a) (1) IA-7
Each authentication operation using the authenticator **SHOULD** require the input of the activation factor. Input of the activation factor **MAY** be accomplished via either direct input on the device or via a hardware connection (e.g., USB, smartcard).	IA-5 (2) (a) (1)
The use of an activation secret by the authenticator **SHALL** meet the requirements of Sec. 5.2.11.	
A biometric activation factor **SHALL** meet the requirements of Sec. 5.2.3, including limits on the number of consecutive authentication failures.	
Submission of the activation factor **SHALL** be a separate operation from unlocking of the host device (e.g., smartphone), although the same activation factor used to unlock the host device **MAY** be used in the authentication operation.	IA-5 (2) (a) (1)
The activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — **SHALL** be zeroized immediately after an authentication transaction has taken place	IA-5 g, IA-5 h. IA-5 (2) (a) (1)

5.1.9.2. Multi-Factor Cryptographic Device Verifiers	
5.2. General Authenticator Requirements	
5.2.1. Physical Authenticators	
CSPs **SHALL** provide subscriber instructions on how to appropriately protect the authenticator against theft or loss.	IA-5 g., IA-5 h., IA-5 (6)
The CSP **SHALL** provide a mechanism to invalidate the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.	IA-5 g., IA-5 h., IA-5 (6)
5.2.2. Rate Limiting (Throttling)	
When required by the authenticator type descriptions in Sec. 5.1, the verifier **SHALL** implement controls to protect against online guessing attacks	
Unless otherwise specified in the description of a given authenticator, the verifier **SHALL** limit consecutive failed authentication attempts on a single subscriber account to no more than 100.	
Additional techniques **MAY** be used to reduce the likelihood that an attacker will lock the legitimate claimant out as a result of rate limiting. These include: ● Requiring the claimant to complete a bot-detection and mitigation challenge before attempting authentication. ● Requiring the claimant to wait following a failed attempt for a period of time that increases as the subscriber account approaches its maximum allowance for consecutive failed attempts (e.g., 30 seconds up to an hour). ● Accepting only authentication requests that come from an allowlist of IP addresses from which the subscriber has been successfully authenticated before. ● Leveraging other risk-based or adaptive authentication techniques to identify user behavior that falls within, or out of, typical norms. These might, for example, include use of IP address, geolocation, timing of request patterns, or	IA-10

browser metadata.	
When the subscriber successfully authenticates, the verifier **SHOULD** disregard any previous failed attempts for that user from the same IP address.	
5.2.3. Use of Biometrics	
Biometrics **SHALL** be used only as part of multi-factor authentication with a physical authenticator (*something you have*).	
The biometric system **SHALL** operate with a false-match rate (FMR) [ISO/IEC2382-37] of 1 in 10000 or better. This FMR **SHALL** be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in [ISO/IEC30107-1].	IA-1 a.1 (b) IA-5 (12)
The biometric system **SHOULD** implement presentation attack detection (PAD).	IA-5 (12) IA-5 (17)
Testing of the biometric system to be deployed **SHOULD** demonstrate at least 90% resistance to presentation attacks for each relevant attack type (i.e., species), where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks.	IA-5 (12) IA-5 (17)
Testing of presentation attack resistance **SHALL** be in accordance with Clause 12 of [ISO/IEC30107-3].	IA-1 a.1 (b) IA-5 (17)
The PAD decision **MAY** be made either locally on the claimant's device or by a central verifier.	IA-5 (17)
The biometric system **SHALL** allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD, meeting the above requirements, is implemented.	IA-5 (12) IA-5 (17)
Once that limit has been reached, the biometric authenticator **SHALL** impose a delay of at least 30 seconds before each subsequent attempt, with an overall limit of no more than 50 consecutive failed authentication attempts (100 if PAD is implemented).	IA-5 (12) IA-5 (17)

Once the overall limit is reached, the biometric system **SHALL** disable biometric user authentication and offer another factor (e.g., a different biometric modality or an activation secret if it is not already a required factor) if such an alternative method is already available.	IA-5 (12)
The verifier **SHALL** make a determination of sensor and endpoint performance, integrity, and authenticity. Acceptable methods for making this determination include, but are not limited to: ● Authentication of the sensor or endpoint ● Certification by an approved accreditation authority ● Runtime interrogation of signed metadata (e.g., attestation) as described in Sec. 5.2.4.	IA-5 (12)
Biometric comparison can be performed locally on the claimant's device or at a central verifier. Since the potential for attacks on a larger scale is greater at central verifiers, comparison **SHOULD** be performed locally.	
If comparison is performed centrally: ● Use of the biometric as an authentication factor **SHALL** be limited to one or more specific devices that are identified using approved cryptography. Since the biometric has not yet unlocked the main authentication key, a separate key **SHALL** be used for identifying the device.	
● Biometric revocation, referred to as biometric template protection in [ISO/IEC24745], **SHALL** be implemented.	IA-1 a.1 (b)
● An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier **SHALL** be established and the sensor or endpoint **SHALL** be authenticated prior to capturing the biometric sample from the claimant.	IA-5 g
● All transmission of biometrics **SHALL** be over an authenticated protected channel.	IA-5 g
Biometric samples collected in the authentication process **MAY** be used to train comparison algorithms or — with user consent — for other research purposes. Biometric samples and any biometric	

data derived from the biometric sample such as a probe produced through signal processing **SHALL** be zeroized immediately after any training or research data has been derived.	
Biometric authentication technologies **SHALL** provide similar performance for subscribers of different demographic types (racial background, gender, ethnicity, etc.).	
5.2.4. Attestation	
An attestation is information conveyed to the verifier regarding a connected authenticator or the endpoint involved in an authentication operation. Information conveyed by attestation **MAY** include, but is not limited to: • The provenance (e.g., manufacturer or supplier certification), health, and integrity of the authenticator and endpoint • Security features of the authenticator • Security and performance characteristics of biometric sensors • Sensor modality	
If this attestation is signed, it **SHALL** be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of [SP800-131A] (112 bits as of the date of this publication).	IA-1 a.1 (b)
Attestation information **MAY** be used as part of a verifier's risk-based authentication decision.	
5.2.5. Phishing (Verifier Impersonation) Resistance	
Approved cryptographic algorithms **SHALL** be used to establish phishing resistance where it is required.	
Keys used for this purpose **SHALL** provide at least the minimum security strength specified in the latest revision of [SP800-131A] (112 bits as of the date of this publication).	IA-1 a.1 (b)
Authenticators that involve the manual entry of an authenticator output, such as out-of-band and OTP authenticators, **SHALL NOT** be considered phishing resistant because the manual entry does not	IA-2(13)

Commented [27]: CSP specific requirement

Commented [29]: Non-Phishing Resistant

Commented [28]: What is the role of these authenticators with regard to the mapping?

bind the authenticator output to the specific session being authenticated. In an AitM attack, an impostor verifier could replay the OTP authenticator output to the verifier and successfully authenticate.	
5.2.5.1. Channel Binding	
An authentication protocol with channel binding **SHALL** establish an authenticated protected channel with the verifier	
It **SHALL** then strongly and irreversibly bind a channel identifier that was negotiated in establishing the authenticated protected channel to the authenticator output (e.g., by signing the two values together using a private key controlled by the claimant for which the public key is known to the verifier).	
The verifier **SHALL** validate the signature or other information used to prove phishing resistance. This prevents an impostor verifier, even one that has obtained a certificate representing the actual verifier, from successfully relaying that authentication on a different authenticated protected channel.	
5.2.5.2. Verifier Name Binding	
An authentication protocol with authenticator name binding **SHALL** establish an authenticated protected channel with the verifier. It **SHALL** then generate an authenticator output that is cryptographically bound to a verifier identifier that is authenticated as part of the protocol.	IA-9
In the case of domain name system (DNS) identifiers, the verifier identifier **SHALL** be either the authenticated hostname of the verifier or a parent domain that is at least one level below the public suffix [PSL] associated with that hostname.	IA-9
The binding **MAY** be established by choosing an associated authenticator secret, by deriving an authenticator secret using the verifier identifier, by cryptographically signing the authenticator output with the verifier identifier, or similar cryptographically secure means.	IA-9

5.2.6. Verifier-CSP Communications	
In situations where the verifier and CSP are separate entities (as shown by the dotted line in [SP800-63] Figure 1), communications between the verifier and CSP **SHALL** occur through a mutually authenticated secure channel (such as a client-authenticated TLS connection) using approved cryptography.	
5.2.7. Verifier Compromise Resistance	
To be considered verifier compromise resistant, public keys stored by the verifier **SHALL** be associated with the use of approved cryptographic algorithms and **SHALL** provide at least the minimum security strength specified in the latest revision of [SP800-131A] (112 bits as of the date of this publication).	IA-8 (4)
Other verifier compromise resistant secrets **SHALL** use approved hash algorithms and the underlying secrets **SHALL** have at least the minimum security strength specified in the latest revision of [SP800-131A] (112 bits as of the date of this publication).	IA-8 (4)
Secrets (e.g., memorized secrets) having lower complexity **SHALL NOT** be considered verifier compromise resistant when hashed because of the potential to defeat the hashing process through dictionary lookup or exhaustive search.	
5.2.8. Replay Resistance	
5.2.9. Authentication Intent	
The goal of authentication intent is to make it more difficult for authenticators (e.g., multi-factor cryptographic devices) to be used without the subject's knowledge, such as by malware on the endpoint. Authentication intent **SHALL** be established by the authenticator itself, although multi-factor cryptographic devices **MAY** establish intent by reentry of the activation factor for the authenticator.	
Authentication intent **MAY** be established in a number of ways. Authentication processes that require the subject's intervention establish intent (e.g., a claimant entering an authenticator output from an OTP device). Cryptographic devices that require user action for each authentication or reauthentication operation also	

establish intent (e.g., pushing a button or reinsertion).	
5.2.10. Restricted Authenticators	
It is the responsibility of the organization to determine the level of acceptable risk for their systems and associated data and to define any methods for mitigating excessive risks. If at any time the organization determines that the risk to any party is unacceptable, then that authenticator **SHALL NOT** be used.	
Further, the risk of an authentication error is typically borne by multiple parties, including the implementing organization, organizations that rely on the authentication decision, and the subscriber. Because the subscriber may be exposed to additional risk when an organization accepts a restricted authenticator and that the subscriber may have a limited understanding of and ability to control that risk, the CSP **SHALL**: 1. Offer subscribers at least one alternate authenticator that is not restricted and can be used to authenticate at the required AAL. 2. Provide meaningful notice to subscribers regarding the security risks of the restricted authenticator and availability of alternatives that are not restricted. 3. Address any additional risk to subscribers in its risk assessment. 4. Develop a migration plan for the possibility that the restricted authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.	
5.2.11. Activation Secrets	
Memorized secrets that are used as an activation factor for a multi-factor authenticator are referred to as *activation secrets*. An activation secret is used to decrypt a stored secret key used for authentication or is compared against a locally held stored verifier to provide access to the authentication key. In either of these cases, the activation secret **SHALL** remain within the authenticator and its associated user endpoint.	IA-5 g.
Authenticators making use of activation secrets **SHALL** require the	IA-5 g.

secrets to be at least 6 characters in length.	
Activation secrets **MAY** be entirely numeric (i.e., a PIN). If alphanumeric (rather than only numeric) values are permitted, all printing ASCII [RFC20] characters as well as the space character **SHOULD** be accepted.	
Unicode [ISO/ISC 10646] characters **SHOULD** be accepted as well in alphanumeric secrets.	
The authenticator **SHALL** contain a blocklist (either specified by specific values or by an algorithm) of at least 10 commonly used activation values and **SHALL** prevent their use as activation secrets.	IA-5 g.
The authenticator or verifier **SHALL** implement a retry-limiting mechanism that effectively limits the number of consecutive failed activation attempts using the authenticator to ten (10).	IA-5 g.
If the entry of an incorrect activation secret causes the authenticator to generate an invalid output that is sent to the central verifier, rate limiting **MAY** be implemented by the verifier	
. In all other cases, rate limiting **SHALL** be implemented in the authenticator.	IA-5 g.
Once the limit of 10 attempts is reached, the authenticator **SHALL** be disabled and a different authenticator **SHALL** be required for authentication.	IA-5 g.
If the authenticator verifies the activation secret locally (rather than using it for decryption of a key), verification **SHALL** be performed within a hardware-based authenticator or in a secure element (e.g., TEE, TPM) that releases the authentication secret only upon presentation of the correct activation secret.	
In other circumstances (i.e., software-based multi-factor authenticators), the authenticator **SHALL** use the memorized secret as a key to decrypt its stored authentication secret. Approved cryptography **SHALL** be used.	

5.2.12. Connected Authenticators	
Cryptographic authenticators require a direct connection between the authenticator and the endpoint being authenticated. This connection **MAY** be wired (e.g., USB or direct connection with a smartcard) or wireless (e.g., NFC, Bluetooth). While in most cases wired connections can be presumed to be secure from eavesdropping and adversary-in-the-middle attacks, additional precautions are required for authenticators that are connected via wireless technologies.	IA-5 g
Wired authenticator connections include both authenticators that are embedded in endpoints (e.g., in a TPM) and those that are connected via an external interface, such as USB. Claimants **SHOULD** be advised to use trusted hardware (cables, etc.) for external connections for additional assurance that they have not been compromised	IA-5 g
Wireless technologies having an effective range of 1 meter or more (e.g., Bluetooth LE) **SHALL** use an authenticated encrypted connection between the authenticator and endpoint.	IA-5 g, IA-5 h.
A pairing process **SHALL** be used to establish a key for encrypted communication between the authenticator and endpoint.	IA-5 g, IA-5 h.
A temporary wired connection between the devices **MAY** also be used to establish the key in lieu of the pairing process.	IA-5 g, IA-5 h.
The pairing process **SHALL** be authenticated through the use of a pairing code.	IA-5 g, IA-5 h.
The pairing code **SHALL** be associated with either the authenticator or endpoint and **SHALL** have at least 20 bits or 6 decimal digits of entropy.	IA-5 g, IA-5 h.
The pairing code **MAY** be printed on the associated device and **SHALL** be conveyed between the devices by manual entry or by using a QR code or similar representation that is optically communicated.	
An example of this is the pairing code used with the virtual contact interface specified in [SP800-73]. The entire authentication	IA-1 a.1 (b)

transaction **SHALL** be encrypted using a key established by the pairing process.	
When a wireless technology with an effective range of less than 1 meter is in use (e.g., NFC), the activation secret, if any, transmitted from the endpoint to authenticator **SHALL** be encrypted using a key established through a pairing process between the devices or through a temporary wired connection.	IA-5 g, IA-5 h.
An authenticated connection using a pairing code meeting the above requirements **SHOULD** be used.	
If the authenticator is configured to require authenticated pairing, pairing code **SHALL** be used.	
The key established as a result of the pairing process **MAY** be either temporary (valid for a limited number of transactions or time) or persistent.	
A mechanism for endpoints to remove persistent keys **SHALL** be provided.	
Where cryptographic operations are required, approved cryptography **SHALL** be used.	
All communication of authentication data between authenticators and endpoints **SHALL** occur directly between those devices or through an authenticated protected channel between the authenticator and endpoint.	
6. Authenticator Lifecycle Management	
6.1. Authenticator Binding	
Authenticators **SHALL** be bound to subscriber accounts either • by issuance by the CSP as part of enrollment or • by registration of a subscriber-provided authenticator that is acceptable to the CSP. These guidelines refer to the *binding* rather than the issuance of an authenticator to accommodate both options.	IA-5 (2) (a) (2) IA-5 (16)

Throughout the digital identity lifecycle, CSPs **SHALL** maintain a record of all authenticators that are or have been associated with each subscriber account.	IA-2 IA-5 (2) (a) (2)
The CSP or verifier **SHALL** maintain the information required for throttling authentication attempts when required, as described in Sec. 5.2.2.	
The CSP **SHALL** also verify the type of user-provided authenticator (e.g., single-factor cryptographic device vs. multi-factor cryptographic device) so verifiers can determine compliance with requirements at each AAL.	
The record created by the CSP **SHALL** contain the date and time the authenticator was bound to the subscriber account.	
The record **SHOULD** include information about the source of the binding (e.g., IP address, device identifier) of any device associated with the enrollment.	
If available, the record **SHOULD** also contain information about the source of unsuccessful authentications attempted with the authenticator.	
When any new authenticator is bound to a subscriber account, the CSP **SHALL** ensure that the binding protocol and the protocol for provisioning the associated keys are done at a level of security commensurate with the AAL at which the authenticator will be used.	IA-5 g.
For example, protocols for key provisioning **SHALL** use authenticated protected channels or be performed in person to protect against adversary-in-the-middle attacks.	IA-5 g.
Binding of multi-factor authenticators **SHALL** require multi-factor authentication or equivalent (e.g., association with the session in which identity proofing has been just completed) be used in order to bind the authenticator. The same conditions apply when a key pair is generated by the authenticator and the public key is sent to the CSP.	

As part of the binding process, the CSP **MAY** require additional information about the new authenticator or the endpoint it is associated with to determine that they are suitable for the AAL being requested and to attempt to determine that the endpoint and authenticator are free from malware.	
6.1.1. Binding at Enrollment	
The CSP **SHALL** bind at least one — and **SHOULD** bind at least two — physical (*something you have*) authenticators to the subscriber account, in addition to a memorized secret or one or more biometric characteristics. Binding of multiple authenticators provides a means to recover from the loss or theft of the subscriber's primary authenticator.	IA-5 (2) (a) (2) IA-5 (16)
If enrollment and binding cannot be completed in a single physical encounter or electronic transaction (i.e., within a single protected session), the following methods **SHALL** be used to ensure that the same party acts as the applicant throughout the processes:	
For remote transactions: 1. The applicant **SHALL** identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.	IA-5 (16)
2. Long-term authenticator secrets **SHALL** only be issued to the applicant within a protected session.	IA-5 g.
For in-person transactions: 1. The applicant **SHALL** identify themselves in person by either using a secret as described in remote transaction (1) above, or through use of a biometric that was recorded during a prior encounter.	IA-5 (16)
2. Temporary secrets **SHALL NOT** be reused.	
3. If the CSP issues long-term authenticator secrets during a	IA-5 (16)

physical transaction, then they **SHALL** be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.	
6.1.2. Post-Enrollment Binding	
6.1.2.1. Binding of an Additional Authenticator at Existing AAL	
With the exception of memorized secrets, CSPs and verifiers **SHOULD** encourage subscribers to maintain at least two valid authenticators of each factor that they will be using.	
For example, a subscriber who usually uses an OTP device as a physical authenticator **MAY** also be issued a number of look-up secret authenticators, or register a device for out-of-band authentication, in case the physical authenticator is lost, stolen, or damaged. See Sec. 6.1.2.3 for more information on replacement of memorized secret authenticators.	
Accordingly, CSPs **SHOULD** permit the binding of additional authenticators to a subscriber account.	
Before adding the new authenticator, the CSP **SHALL** first require the subscriber to authenticate at the AAL (or a higher AAL) at which the new authenticator will be used.	
A separate authentication using existing authenticators **SHALL** be performed following the request to bind a new authenticator, and **SHALL** be valid for 20 minutes.	
When an authenticator is added, the CSP **SHOULD** send a notification to the subscriber via a mechanism that is independent of the transaction binding the new authenticator (e.g., email to an address previously associated with the subscriber).	
The CSP **MAY** limit the number of authenticators that are bound in this manner.	

6.1.2.2. Adding an Additional Factor to a Single-Factor Subscriber Account	
If the subscriber account has only one authentication factor bound to it and an additional authenticator of a different authentication factor is to be added, the subscriber **MAY** request that the subscriber account be upgraded to AAL2	
.Before binding the new authenticator, the CSP **SHALL** require the subscriber to authenticate at AAL1.	
The CSP **SHOULD** send a notification of the event to the subscriber via a mechanism independent of the transaction binding the new authenticator (e.g., email to an address previously associated with the subscriber).	
6.1.2.3. Account Recovery	
If a subscriber that has been identity proofed loses all authenticators necessary to complete authentication, that subscriber **SHALL** repeat the identity proofing process described in [SP800-63A].	IA-1 a.1 (b)
If the CSP has retained information from the evidence used in the original identity proofing process (pursuant to a privacy risk assessment as described in [SP800-63A] Sec. 5.2.2) that is sufficient to perform verification of the subscriber and if that evidence is still valid, it **MAY** repeat only the verification portion of the identity proofing process as described in [SP800-63A].	IA-1 a.1 (b)
The CSP **SHALL** require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing subscriber account.	
Reestablishment of authentication factors at IAL3 **SHALL** be done in person or through a supervised remote process as described in [SP800-63A] Sec. 5.6.8, and **SHALL** perform a successful biometric comparison against the biometric characteristic collected during the original identity proofing process.	IA-1 a.1 (b)
The CSP **SHOULD** send a notification of the event to the subscriber. This **MAY** be the same notice that is required as part of the identity	

proofing process.	
Subscriber accounts that have not been identity proofed (i.e., without IAL) cannot be recovered because there is no reliable means for reassociating the subscriber with that account. Such accounts **SHALL** be treated as abandoned and a new subscriber account **SHALL** be established.	
Replacement of a lost (i.e., forgotten) memorized secret is problematic because it is very common. Additional "backup" memorized secrets do not mitigate this because they are just as likely to also have been forgotten. If a biometric is bound to the subscriber account, the biometric characteristic and associated physical authenticator **SHOULD** be used to establish a new memorized secret.	
As an alternative to the above re-proofing process when there is no biometric bound to the subscriber account, the CSP **MAY** bind a new memorized secret with authentication using two physical authenticators, along with a confirmation code that has been sent to one of the subscriber's addresses of record.	
The confirmation code **SHALL** consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP800-90Ar1].	IA-1 a.1 (b)
Confirmation codes **SHALL** be valid for at most: ● 21 days, when sent to a postal address of record within the contiguous United States; ● 30 days, when sent to a postal address of record outside the contiguous United States; ● 10 minutes, when sent to a telephone of record (SMS or voice); or ● 24 hours, when sent to an email address of record.	
6.1.2.4. External Authenticator Binding	
The binding process **MAY** begin with a request from an endpoint that has authenticated to the CSP obtaining a binding code from the CSP that is input into the endpoint associated with the new authenticator and sent to that CSP.	IA-5 (10)

Alternatively, the endpoint associated with the new authenticator **MAY** obtain a binding code from the CSP, which is input to an authenticated endpoint and sent to the CSP.	IA-5 (10)
In addition to the requirements given in Sec. 6.1.2.1, Sec. 6.1.2.2, and Sec. 6.1.2.3 above as applicable, the following requirements **SHALL** apply when binding an external authenticator: • An authenticated protected session **SHALL** be established by the endpoint associated with the new authenticator and the CSP.	IA-5 g.
• The subscriber **MAY** be prompted to enter an identifier by which they are known by the CSP on the endpoint associated with the new authenticator.	
• The CSP **SHALL** generate a *binding code* using an approved random number generator and send it to either the new authenticator endpoint or the authenticated endpoint approving the binding. The binding code **SHALL** have at least 40 bits of entropy if used in conjunction with an identifier entered on the previous step; otherwise a binding code with at least 112 bits of entropy **SHALL** be required.	
• The subscriber **SHALL** transfer the binding code to the other endpoint. This transfer **SHALL** be either manual or via a local out-of-band method such as a QR code. The binding code **SHALL NOT** be communicated over any insecure channel such as email or PSTN (SMS or voice).	
• The binding code **SHALL** be usable only once and **SHALL** be valid for a maximum of 10 minutes.	
• Following the binding of the new authenticator (or issuance of a certificate, in the case of PKI-based authenticators), the CSP **SHOULD** encourage the subscriber to authenticate with the new authenticator to confirm that the process has completed successfully.	
• The CSP **SHALL** provide clear instruction on what the subscriber should do in the event of an authenticator binding mishap, such as a button or contact address to allow a mis-	IA-5 g.

bound authenticator to be quickly invalidated as appropriate. This **MAY** be provided in the authenticated session or in the binding notification described in Sec. 6.1.2.1, Sec. 6.1.2.2, and Sec. 6.1.2.3 above.	
6.1.3. Binding to a Subscriber-provided Authenticator	
CSPs **SHOULD**, where practical, accommodate the use of subscriber-provided authenticators in order to relieve the burden to the subscriber of managing a large number of authenticators	IA-5 (10)
Binding of these authenticators **SHALL** be done as described in Sec. 6.1.2.	IA-5 (10)
In situations where the authenticator strength is not self-evident (e.g., between single-factor and multi-factor authenticators of a given type), the CSP **SHALL** assume the use of the weaker authenticator unless it is able to establish that the stronger authenticator is in fact being used (e.g., by verification with the issuer or manufacturer of the authenticator).	
6.1.4. Renewal	
The subscriber **SHOULD** bind a new or updated authenticator an appropriate amount of time before an existing authenticator's expiration.	IA-5 f.
The process for this **SHOULD** conform closely to the binding process for an additional authenticator described in Sec. 6.1.2.1. The CSP **MAY** periodically take other actions, such as reconfirming address of record, either as a part of the renewal process or separately.	
Following successful use of the replacement authenticator, the CSP **MAY** invalidate the authenticator that is expiring.	
6.2. Loss, Theft, Damage, and Unauthorized Duplication	
Suspension, revocation, or destruction of compromised authenticators **SHOULD** occur as promptly as practical following detection.	

Commented [30]: Is this related to IA-5 f. (changing or refreshing an authenticator)?

Organizations **SHOULD** establish time limits for this process.	
To facilitate secure reporting of the loss, theft, or damage to an authenticator, the CSP **SHOULD** provide the subscriber with a method of authenticating to the CSP using a backup or alternate authenticator.	
This backup authenticator **SHALL** be either a memorized secret or a physical authenticator. Either could be used, but only one authentication factor is required to make this report.	
Alternatively, the subscriber **MAY** establish an authenticated protected channel to the CSP and verify information collected during the proofing process..	
The CSP **MAY** choose to verify an address of record (i.e., email, telephone, postal) and suspend authenticators reported to have been compromised.	
The suspension **SHALL** be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.	
The CSP **MAY** set a time limit after which a suspended authenticator can no longer be reactivated	
6.3. Expiration	
CSPs **MAY** issue authenticators that expire. If and when an authenticator expires, it **SHALL NOT** be usable for authentication.	
When an authentication is attempted using an expired authenticator, the CSP **SHOULD** give an indication to the subscriber that the authentication failure is due to expiration rather than some other cause.	
The CSP **SHALL** require subscribers to surrender or prove destruction of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.	

6.4. Invalidation	
CSPs SHALL invalidate authenticators promptly when a subscriber account ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.	
The CSP SHALL require subscribers to surrender or certify destruction of any physical authenticator containing subscriber attributes, such as certificates signed by the CSP, as soon as practical after invalidation takes place.	
7. Session Management	
To facilitate this behavior, a *session* MAY be started in response to an authentication event, and continue the session until such time that it is terminated.	
The session MAY be terminated for any number of reasons, including but not limited to an inactivity timeout, an explicit logout event, or other means.	
The session MAY be continued through a reauthentication event — described in Sec. 7.2 — wherein the subscriber repeats some or all of the initial authentication event, thereby re-establishing the session.	
7.1. Session Bindings	
A session secret SHALL be shared between the subscriber's software and the service being accessed.	
This secret binds the two ends of the session, allowing the subscriber to continue using the service over time.	
The secret SHALL be presented directly by the subscriber's software or possession of the secret SHALL be proven using a cryptographic mechanism.	
Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of	

Commented [31]: CSP specific requirement

authentication and optionally refreshed during the session. The nature of a session depends on the application, such as: ● a web browser session with a “session” cookie, or ● an instance of a mobile application that retains a session secret.	
Session secrets **SHALL NOT** be persistent (retained across a restart of the associated application or a reboot of the host device).	
The secret used for session binding **SHALL** be generated by the session host in direct response to an authentication event.	
A session **SHOULD** inherit the AAL properties of the authentication event which triggered its creation.	
A session **MAY** be considered at a lower AAL than the authentication event but **SHALL NOT** be considered at a higher AAL than the authentication event.	
Secrets used for session binding **SHALL** meet all of the following requirements: 1. Secrets are generated by the session host during an interaction, typically immediately following authentication. 2. Secrets are generated by an approved random bit generator [SP800-90Ar1] and contain at least 64 bits of entropy. 3. Secrets are erased or invalidated by the session subject when the subscriber logs out. 4. Secrets are sent to and received from the device using an authenticated protected channel. 5. Secrets will time out and are not accepted after the times specified in Sections 4.1.3, 4.2.3, and 4.3.3, as appropriate for the AAL. 6. Secrets are not made available to insecure communications between the host and subscriber’s endpoint.	IA-1 a.1 (b)
In addition, secrets used for session binding **SHOULD** be erased on the subscriber endpoint when they log out or when the secret is deemed to have expired.	
They **SHOULD NOT** be placed in insecure locations such as HTML5 Local Storage due to the potential exposure of local storage to	

cross-site scripting (XSS) attacks.	
Authenticated sessions **SHALL NOT** fall back to an insecure transport, such as from https to http, following authentication.	
URLs or POST content **SHALL** contain a session identifier that **SHALL** be verified by the RP to protect against cross-site request forgery.	
7.1.1. Browser Cookies	
Cookies used for session maintenance **SHALL** meet all of the following requirements: 1. Cookies are tagged to be accessible only on secure (HTTPS) sessions. 2. Cookies are accessible to the minimum practical set of hostnames and paths.	
In addition, session maintenance cookies **SHOULD** be tagged to be inaccessible via JavaScript (HttpOnly).	
They **SHOULD** contain only an opaque string (such as a session identifier), and **SHOULD NOT** contain cleartext PII.	
They **SHOULD** be tagged to expire at, or soon after, the session's validity period.	
This latter requirement is intended to limit the accumulation of cookies, but **SHALL NOT** be depended upon to enforce session timeouts.	
7.1.2. Access Tokens	
The presence of an OAuth access token **SHALL NOT** be interpreted by the RP as presence of the subscriber, in the absence of other signals.	
The OAuth access token, and any associated refresh tokens, **MAY** be valid long after the authentication session has ended and the subscriber has left the application.	

7.1.3. Device Identification	
Other methods of secure device identification — including but not limited to mutual TLS, token binding, or other mechanisms — **MAY** be used to enact a session between a subscriber and a service.	
7.2. Reauthentication	
Periodic reauthentication of sessions **SHALL** be performed to confirm the continued presence of the subscriber at an authenticated session (i.e., that the subscriber has not walked away without logging out).	IA-11
A session **SHALL NOT** be extended past the guidelines in Sections 4.1.3, 4.2.3, and 4.3.3 (depending on AAL) based on presentation of the session secret alone. Prior to session expiration, the reauthentication time limit **SHALL** be extended by prompting the subscriber for the authentication factors specified in Table 2.	
When a session has been terminated, due to a time-out or other action, the subscriber **SHALL** be required to establish a new session by authenticating again.	

7.2.1. Reauthentication from a Federation or Assertion	
8. Threats and Security Considerations (Informative)	
8.1. Authenticator Threats (Informative)	
8.2. Threat Mitigation Strategies (Informative)	
8.3. Authenticator Recovery (Informative)	
8.4. Session Attacks (Informative)	
9. Privacy Considerations (Informative)	
9.1. Privacy Risk Assessment (Informative)	
9.2. Privacy Controls (Informative)	
9.3. Use Limitation (Informative)	
9.4. Agency-Specific Privacy Compliance (Informative)	
10. Usability Considerations (Informative)	
10.1. Usability Considerations Common to Authenticators (Informative)	
10.2. Usability Considerations by Authenticator Type (Informative)	
10.2.1. Memorized Secrets (Informative)	
10.2.2. Look-Up Secrets (Informative)	
10.2.3. Out-of-Band (Informative)	
10.2.4. Single-Factor OTP Device (Informative)	
10.2.5. Multi-Factor OTP Device (Informative)	
10.2.6. Single-Factor Cryptographic Software (Informative)	
10.2.7. Single-Factor Cryptographic Device (Informative)	
10.2.8. Multi-Factor Cryptographic Software (Informative)	

10.2.9. Multi-Factor Cryptographic Device (Informative)	
10.3. Summary of Usability Considerations (Informative)	
10.4. Biometrics Usability Considerations (Informative)	
11. Equity Considerations (Informative)	

800-63C-4

NIST 800-63C Reference	800-53 rev 5 control
1. Purpose (Informative)	
2. Introduction (Informative)	
3. Definitions and Abbreviations (Informative)	
4. Federation Assurance Level (FAL)	
At all FALs, all assertions **SHALL** be used with a federation protocol as described in Sec. 5.	IA-8 (4)
All assertions **SHALL** comply with the detailed requirements in Sec. 6.	IA-8 (4)
All assertions **SHALL** be presented using one of the methods described in Sec. 7. Examples of assertions used in federated protocols include the ID Token in OpenID Connect [OIDC] and assertions written in the Security Assertion Markup Language [SAML].	
At all FALs, the IdP **SHALL** employ appropriately tailored security controls (to include control enhancements) from the moderate or high baseline of security controls defined in [SP800-53] or equivalent federal (e.g., [FEDRAMP]) or industry standard.	IA-1 a.1 (b)
4.1. Federation Assurance Level 1 (FAL1)	
At FAL1, the assertion being generated by the IdP **SHALL** meet a core set of requirements defined in Sec. 6, including protection against modification or construction by an attacker by having the assertion contents signed by the IdP using approved cryptography.	IA-8 (4)
An RP **SHALL** verify the origin and integrity of the assertion upon receipt, as discussed in Sec. 6, ensuring that the assertion has originated from the expected source.	

All assertions at FAL1 **SHALL** be audience-restricted to a specific RP or set of RPs, and the RP **SHALL** validate that it is one of the targeted RPs for the given assertion.	
The IdP **SHALL** ensure that any party holding the assertion, including the RP, is unable to impersonate the IdP at a non-targeted RP by protecting the assertion with a signature and key using approved cryptography.	
If the assertion is protected by a digital signature using an asymmetric key, the IdP **MAY** use the same public and private key pair to sign assertions to multiple RPs.	
The IdP **MAY** publish its public key in a verifiable fashion, such as at an HTTPS-protected URL at a well-known location. If the assertion is protected by a keyed message authentication code (MAC) using a shared key, the IdP **SHALL** use a different shared key for each RP.	
At FAL1, the trust agreement between the IdP and RP **MAY** be established entirely dynamically.	
4.2. Federation Assurance Level 2 (FAL2)	
At FAL2, the assertion **SHALL** also be strongly protected from being injected by an attacker. To accomplish this, the assertion **SHOULD** be presented using back channel presentation as discussed in Sec. 7.1, as in the OpenID Connect Basic Client profile [OIDC-Basic].	IA-8 (4)
If front channel presentation is used as discussed in Sec. 7.2, additional injection protections **SHALL** be implemented by the RP.	
At FAL2, the trust agreement between the IdP and RP **SHALL** be established statically, including establishing limits of which attributes are made available to the RP and for what purpose	
This trust agreement **MAY** be bilateral between the IdP and RP or **MAY** be managed through the use of a multilateral federation partnership.	

The registration **MAY** be dynamic, provided that the RP and IdP can prove their connection at runtime to the established trust agreement between them. Such methods for this proof vary by federation protocol, but can include presentation of software attestations and proof of control over URLs at trusted domains	
Government-operated IdPs asserting authentication at FAL2 **SHALL** protect keys used for signing or encrypting those assertions with mechanisms validated at [FIPS140] Level 1 or higher.	IA-1 a.1 (b)
4.3. Federation Assurance Level 3 (FAL3)	
At FAL3, the subscriber **SHALL** authenticate to the RP by presenting an authenticator directly to the RP in addition to presenting an assertion. The authenticator presented is known as a *bound authenticator*, described in Sec. 6.1.2.	
At FAL3, the trust agreement and registration between the IdP and RP **SHALL** be established statically.	
All identifying key material and federation parameters for all parties (including the list of attributes sent to the RP) **SHALL** be fixed ahead of time, before the federated authentication process can take place.	IA-
Runtime decisions **MAY** be used to further limit what is sent between parties in the federated authentication process (e.g., a runtime decision could opt to not disclose an email address even though this attribute was included in the parameters of the trust agreement).	
IdPs asserting authentication at FAL3 **SHALL** protect keys used for signing or encrypting those assertions with mechanisms validated at [FIPS140] Level 1 or higher.	IA-1 a.1 (b)
4.4. Requesting and Processing xALs	

The RP **SHALL** be informed of the following information for each federated transaction: ● The IAL of the subscriber account being presented to the RP, or an indication that no IAL claim is being made ● The AAL of the currently active session of the subscriber at the IdP, or an indication that no AAL claim is being made ● The FAL of the federated transaction	
The RP gets this xAL information from a combination of parameters in the trust agreement as described in Sec. 5.1 and information included in the assertion as described in Sec. 6. If the xAL is unchanging for all messages between the IdP and RP, the xAL information **SHALL** be included in the parameters of the trust agreement between the IdP and RP.	
If the xAL varies, the information **SHALL** be included as part of the assertion as discussed in Sec. 6.	
The IdP **MAY** indicate that no claim is made to the IAL or AAL for a given federation transaction. In such cases, no default value is assigned to the resulting xAL.	
The RP **SHALL** determine the minimum IAL, AAL, and FAL it is willing to accept for access to any offered functionality.	IA-12 a., IA-12 (6)
An RP **MAY** vary its functionality based on the IAL, AAL, and FAL of a specific federated authentication.	
In a federation process, only the IdP has direct access to the details of the subscriber account, which determines the applicable IAL, and the authentication event at the IdP, which determines the applicable AAL. Consequently, the RP **SHALL** consider the IdP's declaration of the IAL and AAL as the sole source of these levels for a given federated transaction.	
The RP **SHALL** ensure that the federation transaction meets the requirements of the FAL declared in the assertion.	

IdPs **SHALL** support a mechanism for RPs to specify a set of minimum acceptable xALs as part of the trust agreement and **SHOULD** support the RP specifying a more strict minimum set at runtime as part of the federation transaction.	
When an RP requests a particular xAL, the IdP **SHOULD** fulfill that request, if possible, and **SHALL** indicate the resulting xAL in the assertion.	
5. Federation	
5.1. Trust Agreements	
Trust agreements SHALL establish the following parameters: ● The set of attributes the IdP can make available to the RP ● The population of subscriber accounts the IdP can create assertions for ● The set of attributes the RP will request (a subset of the attributes made available) ● The purpose for each attribute requested by the RP ● The authorized party responsible for decisions regarding the release of subscriber attributes ● The means of informing subscribers about attribute release to the RP ● The xALs available from the IdP ● The xALs required by the RP	IA-1 a.1 (a) IA-4(6) IA-8 (2) (b)
Trust agreements are able to be established either statically or dynamically. In a static establishment, there is often a legal or contractual agreement binding the parties to a set of expected behaviors, rights, and requirements. The parameters of static trust agreements SHALL be available to all parties in the agreement, including the operator of the IdP, the operator of the RP, and affected subscribers.	IA-4(6)
The parameters of a dynamic trust agreement SHALL be disclosed to the subscriber by the RP and the IdP during the federation transaction.	IA-4(6)

For a static trust agreement, the authorized party MAY be the organization responsible for the IdP. In this case, consent to release attributes is decided for all subscribers and established by an allowlist as described in Sec. 5.3.1, allowing for the disclosure of attribute information without direct decisions and involvement by the subscriber.	
A static trust agreement MAY stipulate that an individual, such as the subscriber, is to be prompted at runtime for consent to disclose attributes as discussed in Sec. 5.3.3. Since dynamic trust agreements are established by subscriber actions, the authorized party in a dynamic trust agreement is always the subscriber.	
Disclosure of attributes in dynamic trust agreements SHALL be subject to a runtime decision from the subscriber and SHALL NOT be subject to an allowlist at the IdP.	
During the course of a single federation transaction, it is important for the policies and expectations of the IdP and RP to be unambiguous for all parties involved. Therefore, there **SHOULD** be only one set of trust agreements in effect for a given transaction. This will usually be determined by the unique pair consisting of a single IdP and a single RP. However, these agreements could vary in other ways, such as an IdP and RP having different agreements for different populations of subscribers.	IA-1 a.1 (a) IA-4(6)
5.1.1. Bilateral Trust Agreements	
The IdP **SHALL** disclose its supported IAL, AAL, and FAL levels to the RP.	
The IdP **MAY** disclose a subset of its capabilities to a given RP depending on the needs of the application, for example only disclosing to a low-risk RP that accounts are proofed at IAL1 or better.	
The RP **SHALL** disclose its list of required attributes to the IdP, including its purpose for use of each requested attribute.	

The RP **SHALL** communicate its required IAL, AAL, and FAL to the IdP, including whether no claim is required for IAL or AAL.	IA-1 a.1 (a)
The IdP **SHALL** transmit only those attributes that were explicitly requested by the RP.	
RPs **SHALL** include their requested attributes in their privacy risk assessment.	IA-1 a.1 (a)
5.1.2. Multilateral Trust Agreements	
Federation authorities **SHALL** establish parameters regarding expected and acceptable IALs, AALs, and FALs in connection with the federated relationships they enable.	IA-1 a.1 (a) IA-4(6) IA-8 (4)
Federation authorities **SHALL** individually vet each participant in the federation to determine whether they adhere to their expected standards.	IA-4(6)
Vetting of IdPs and RPs **SHALL** establish, as a minimum, that: ● Assertions generated by IdPs adhere to the requirements in Sec. 6. ● RPs adhere to requirements for handling subscriber attribute data, such as retention, aggregation, and disclosure to third parties. ● RP and IdP systems use approved profiles of federation protocols.	IA-1 a. 1 (a) IA-4(6)
Federation authorities **MAY** assist the technical connection and configuration process between members, such as by publishing configuration data for IdPs or by issuing software statements for RPs.	
Most federations managed through authorities have a simple membership model: parties are either in the federation or they are not. More sophisticated federations **MAY** have multiple membership tiers that federated parties can use to tell whether other parties in the federation have been more thoroughly vetted.	

IdPs **MAY** decide that certain subscriber attributes are only releasable to RPs in higher tiers and RPs **MAY** decide to accept certain information only from IdPs in higher tiers.	
5.1.3. Proxied Federation	
Where proxies are used, they function as an IdP on one side and an RP on the other. Therefore, all normative requirements that apply to IdPs and RPs **SHALL** apply to proxies in their respective roles.	
Federations presented through a proxy **SHALL** be represented by the lowest FAL used during the proxied transaction. For example, if a proxy takes in an assertion from the IdP at FAL2 but presents a downstream assertion to the RP at FAL1, the entire transaction is considered FAL1	
Likewise if a federation takes in an assertion at FAL1 but presents a downstream assertion to the RP at FAL3, the entire transaction is still considered FAL1. The proxy **SHALL** communicate this aspect to the RP either at runtime or through pre-configuration as part of the trust agreement.	
5.2. Registration	
5.2.1. Manual Registration	
IdPs and RPs **MAY** act as their own authorities on who to federate with as in Sec. 5.1.1 or **MAY** externalize those authority decisions to an external party as in Sec. 5.1.2.	
Protocols requiring the transfer of keying information **SHALL** use a secure method during the registration process to exchange keying information needed to operate the federated relationship, including any shared secrets or public keys.	
Any symmetric keys used in this relationship **SHALL** be unique to a pair of federation participants.	
Federation relationships **SHALL** establish parameters regarding expected and acceptable IALs and AALs in connection with the federated relationship.	

5.2.2. Dynamic Registration	
This process allows IdPs and RPs to be connected together without manually establishing a connection between them using manual registration (See Sec. 5.2.1). IdPs that support dynamic registration **SHALL** make their configuration information (such as dynamic registration endpoints) available in such a way as to minimize system administrator involvement.	
5.3. Authentication and Attribute Disclosure	
Once the IdP and RP have entered into a trust agreement and have completed registration, the federation protocol can be used to pass subscriber attributes from the IdP to the RP. The decision of whether an authentication can occur or attributes may be passed **SHALL** be determined by the authorized party stipulated by the trust agreement, through use of an allowlist, a blocklist, or a runtime decision.	
A subscriber's attributes **SHALL** be transmitted between IdP and RP only for identity federation transactions or support functions such as identification of compromised subscriber accounts as discussed in Sec. 5.5. A subscriber's attributes are not to be transmitted for any other purposes, even when parties are allowlisted.	
A subscriber's attributes **SHALL NOT** be used by the RP for purposes other than those stipulated in the trust agreement.	
The subscriber **SHALL** be informed of the transmission of attributes to an RP.	
In the case where the authorized party is the organization, the organization **SHALL** make available to the subscriber the list of approved RPs and the associated sets of attributes sent to those RPs.	
In the case where the authorized party is the subscriber, the subscriber **SHALL** be prompted prior to release of attributes using a runtime decision at the IdP as described in Sec. 5.3.3.	

The IdP **SHALL** provide effective mechanisms for redress of subscriber complaints or problems (e.g., subscriber identifies an inaccurate attribute value). See Sec. 10 on usability considerations for redress.	
5.3.1. IdP Allowlists of RPs	
In a static trust agreement, IdPs **MAY** establish allowlists of RPs authorized to receive authentication and attributes from the IdP without a runtime decision from the subscriber. .	
When placing an RP on its allowlist, the IdP **SHALL** ensure that the RP abides by all applicable provisions and requirements in the SP 800-63 guidelines.	
The IdP **SHALL** determine which identity attributes are passed to the allowlisted RP upon authentication. IdPs **SHALL** make allowlists available to subscribers as described in Sec. 9.2.	
IdP allowlists **SHALL** uniquely identify RPs through the means of domain names, cryptographic keys, or other identifiers applicable to the federation protocol in use	
Any entities that share an identifier **SHALL** be considered equivalent for the purposes of the allowlist. For example, a wildcard domain identifier of “*.example.com” would match the domains “www.example.com”, “service.example.com”, and “unknown.example.com” equally. All three of these sites would be treated as the same RP for disclosure decisions using the allowlist.	
Allowlists **SHOULD** be as specific as possible to avoid unintentional impersonation of an RP.	
5.3.2. IdP Blocklists of RPs	
IdPs **MAY** establish blocklists of RPs not authorized to receive authentication assertions or attributes from the IdP, even if requested to do so by the subscriber.	
If an RP is on an IdP’s blocklist, the IdP **SHALL NOT** produce an assertion targeting the RP in question under any circumstances.	

IdP blocklists **SHALL** uniquely identify RPs through the means of domain names, cryptographic keys, or other identifiers applicable to the federation protocol in use.	
Any entities that share an identifier **SHALL** be considered equivalent for the purposes of the blocklist. For example, a wildcard domain identifier of "*.example.com" would match the domains "www.example.com", "service.example.com", and "unknown.example.com" equally. All three of these sites would be treated as the same RP for decisions using the blocklist.	
5.3.3. IdP Runtime Decisions	
Every RP that is in a trust agreement with an IdP but not on an allowlist or a blocklist with that IdP **SHALL** be governed by a default policy in which runtime authorization decisions will be made by an authorized party identified by the trust agreement.	
The IdP **SHALL** provide the authorized party with explicit notice and prompt them for positive confirmation before any attributes about the subscriber are transmitted to the RP.	
At a minimum, the notice **SHOULD** be provided by the party in the position to provide the most effective notice and obtain confirmation, consistent with Sec. 9.2.	
The IdP **SHALL** disclose which attributes will be released to the RP if the transaction is approved.	
If the federation protocol in use allows for optional attribute disclosure at runtime, the authorized party **SHALL** be given the option to decide whether to transmit specific attributes to the RP without terminating the federation transaction entirely.	
To mitigate the risk of unauthorized exposure of sensitive information (e.g., shoulder surfing), the IdP **SHALL**, by default, mask sensitive information displayed to the authorized party.	

If the authorized party is the subscriber, the IdP **SHALL** provide mechanisms for the subscriber to temporarily unmask such information in order for the subscriber to view full values before transmission. For more details on masking, see Sec. 10 on usability considerations.	
An IdP **MAY** employ mechanisms to remember and re-transmit the exact attribute bundle to the same RP, remembering the authorized party's decision. This mechanism is associated with the subscriber account as managed by the IdP.	
If such a mechanism is provided, the IdP **SHALL** allow the authorized party to revoke such remembered access at a future time.	
5.3.4. RP Allowlists of IdPs	
RPs **MAY** establish allowlists of IdPs from which the RP will accept authentication and attributes without a runtime decision from the subscriber.	
When placing an IdP in its allowlist, the RP **SHALL** ensure that the IdP abides by the provisions and requirements in these guidelines.	
RP allowlists **SHALL** uniquely identify IdPs through the means of domain names, cryptographic keys, or other identifiers applicable to the federation protocol in use.	
5.3.5. RP Blocklists of IdPs	
RPs **MAY** also establish blocklists of IdPs that the RP will not accept authentication or attributes from, even when requested by the subscriber. A blocklisted IdP can be otherwise in a valid trust agreement with the RP, for example if both are under the same federation authority.	
RP blocklists **SHALL** uniquely identify IdPs through the means of domain names, cryptographic keys, or other identifiers applicable to the federation protocol in use.	

5.3.6. RP Runtime Decisions	
Every IdP that is in a trust agreement with an RP but not on an allowlist or a blocklist with that RP **SHALL** be governed by a default policy in which runtime authorization decisions will be made by the authorized party indicated in the trust agreement.	
The RP **MAY** employ mechanisms to remember the authorized party's decision to use a given IdP. Since this mechanism is employed prior to authentication at the RP, the manner in which the RP provides this mechanism (e.g., a browser cookie outside the authenticated session) is separate from the RP subscriber account described in Sec. 5.4.	
If such a mechanism is provided, the RP **SHALL** allow the authorized party to revoke such remembered options at a future time.	
5.4. RP Subscriber Accounts	
The RP subscriber account **SHALL** be bound to at least one federated identifier, and a given federated identifier is bound to only one RP subscriber account at a given RP.	IA-4 b., IA-4 c., IA-8
An RP subscriber account is *terminated* when the RP removes all access to the account at the RP. Termination **SHALL** include unbinding any federated identifiers and bound authenticators as well as removing attributes and information associated with the account except what is required for auditing and security purposes.	
An RP **MAY** terminate an RP subscriber account independently from the IdP for a variety of reasons, regardless of the current validity of the subscriber account from which it is derived.	
An authenticated session **SHALL** be created by the RP only when the RP has processed and verified a valid assertion from the IdP that is the issuer of the federated identifier associated with the RP subscriber account.	IA-8
If the assertion also requires presentation of a bound authenticator at FAL3, the bound authenticator **SHALL** also be presented and processed before the RP subscriber account is associated with an	IA-8

authenticated session, as discussed in Sec. 6.1.2.	
5.4.1. Provisioning Models	
The lifecycle of the provisioning process for an RP subscriber account varies depending on factors including the trust agreement discussed in Sec. 5.1 and the deployment pattern of the IdP and RP. However, in all cases, the RP subscriber account **SHALL** be provisioned at the RP prior to the establishment of an authenticated session at the RP in one of the following ways:	
Just-In-Time Provisioning An RP subscriber account is created automatically the first time the RP receives an assertion with an unknown federated identifier from an IdP. Any identity attributes learned during the federation process, either within the assertion or through an identity API as discussed in Sec. 6.3, **MAY** be associated with the RP subscriber account. Accounts provisioned in this way are bound to the federated identifier in the assertion used to provision them. This is the most common form of provisioning in federation systems, as it requires the least coordination between the RP and IdP. However, in such systems, the RP **SHALL** be responsible for managing any cached attributes it might have.	IA-4 b., IA-4 c., IA-4(5)
Pre-provisioning An RP subscriber account is created by the IdP pushing the attributes to the RP or the RP pulling attributes from the IdP. Pre-provisioning of accounts generally occurs in bulk through a provisioning API as discussed in Sec. 5.4.3, as the provisioning occurs prior to the represented subscribers authenticating through a federated transaction. Pre-provisioned accounts **SHALL**	IA-4 b., IA-4 c.

be bound to a federated identifier at the time of provisioning. Any time a particular federated identifier is seen by the RP, the associated account can be logged in as a result. This form of provisioning requires infrastructure and planning on the part of the IdP and RP, but these processes can be facilitated by automated protocols. The RP also collects attributes about users who have not interacted with the RP system yet, which can cause privacy issues. Additionally, the IdP and RP must keep the set of provisioned accounts synchronized over time as discussed in Sec. 5.4.2.	
Other RP subscriber account provisioning models are possible but the details of such models are outside the scope of these guidelines. The details of any alternative provisioning model **SHALL** be included in the privacy risk assessments of the IdP and RP.	
All organizations **SHALL** document their provisioning model as part of their trust agreement.	
5.4.2. Attribute Synchronization	
From the RP's perspective, the IdP is the authoritative source for any attributes that the IdP asserts as being associated with the subscriber account at the IdP. However, the RP **MAY** additionally collect, and optionally verify, other attributes to associate with the RP subscriber account. Sometimes, these attributes can even override what's asserted by the IdP. For example, if an IdP asserts a full display name for the subscriber, the RP can allow the subscriber to provide an alternative preferred name for use at the RP.	IA-4(9)
The IdP **SHOULD** signal downstream RPs when the attributes of a subscriber account available to the RP have been updated. This can be accomplished using shared signaling as described in Sec.	IA-4(9)

5.7, through a provisioning API as described in Sec. 5.4.3, or by providing a signal in the assertion (e.g., a timestamp indicating when relevant attributes were last updated, allowing the RP to determine that its cache is out of date).	
The IdP **SHOULD** signal downstream RPs when a subscriber account is terminated, or when the subscriber account's access to an RP is revoked. This can be accomplished using shared signaling as described in Sec. 5.7 or through a provisioning API as described in Sec. 5.4.3. Upon receiving such a signal, the RP **SHALL** terminate the RP subscriber account and remove all personal information associated with the RP subscriber account, except what is required for audit and security purposes.	
5.4.3. Provisioning APIs	
The attributes in the provisioning API available to a given RP **SHALL** be limited to only those necessary for the RP to perform its functions.	
As part of establishing the trust agreement, the IdP **SHALL** document when an RP is given access to a provisioning API including at least the following: ● the purpose for the access using the provisioning model; ● the set of attributes made available to the RP; ● whether the API functions as a push to the RP, a pull from the RP, or both; and ● the population of subscribers whose attributes are made available to the RP.	
The IdP **SHALL** require authentication from the RP for any pull-based access to a provisioning API. The RP **SHALL** require authentication from the IdP for any push-based access to a provisioning API.	
A provisioning API **SHALL NOT** be made available under a dynamic or implicit trust agreement.	
The IdP **SHALL NOT** make a provisioning API available to any RP outside of an established trust agreement.	

The IdP **SHALL** provide access to a provisioning API only as part of a federated identity relationship with an RP to facilitate federated transactions with that RP and related functions such as signaling revocation of the subscriber account.	
The IdP **SHALL** revoke an RP's access to the provisioning API once access is no longer required by the RP for its functioning purposes or when the trust agreement is terminated.	
Any provisioning API provided to the RP **SHALL** be under the control and jurisdiction of the IdP.	
External attribute providers **MAY** be used as information sources by the IdP to provide attributes through this provisioning API, but the IdP is responsible for the content and accuracy of the information provided by the referenced attribute providers.	
When a provisioning API is in use, the IdP **SHALL** signal to the RP when a subscriber account has been terminated.	
When receiving such a signal, the RP **SHALL** terminate the associated RP subscriber account.	
5.4.4. Attribute Collection	
The RP **MAY** collect and maintain additional attributes from the subscriber beyond those provided by the IdP. These attributes are governed separately from any federation agreement since they are collected directly by the RP.	
All attributes associated with an RP subscriber account, regardless of their source, **SHALL** be removed when the RP subscriber account is terminated.	
The RP **SHALL** disclose to the subscriber the purpose for collection of any additional attributes.	
These attributes **SHALL** be used solely for the stated purposes of the RP's functionality and **SHALL NOT** have any secondary use, including communication of said attributes to other parties.	

An RP **SHALL** disclose any additional attributes collected, and their use, as part of its System of Records Notice (SORN).	
The RP **SHALL** provide an effective means of redress for the subscriber to update and remove these additionally-collected attributes from the RP subscriber account. See Sec. 10 on usability considerations for redress.	
5.4.5. Time-based Removal of RP Subscriber Accounts	
Over time, an RP could accumulate RP subscriber accounts that are no longer accessible from the IdP. This poses a risk to the RP for holding personal information in the RP subscriber accounts, especially when a just-in-time provisioning model is in use and no shared signaling is available from the IdP to signal subscriber account termination as discussed in Sec. 5.7. In such circumstances, the RP **SHOULD** employ a time-based mechanism to identify RP subscriber accounts for termination that have not been accessed after a period of time, for example, 120 days since last access.	
When processing such an inactive account, the RP **SHALL** provide sufficient notice to the subscriber, if possible, about the pending termination of the account and provide the subscriber with an option to re-activate the account prior to its scheduled termination.	
Upon termination, the RP **SHALL** remove all personal information associated with the RP subscriber account, except what is required for audit and security purposes.	
5.5. Privacy Requirements	
If an IdP discloses information on subscriber activities at an RP to any party, or processes the subscriber's attributes for any purpose other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, to comply with law or legal process, or, in the case of a specific user request, to transmit the information, the IdP **SHALL** implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.	
Measures **MAY** include providing clear notice, obtaining subscriber	

consent, or enabling selective use or disclosure of attributes.	
When an IdP uses consent measures, the IdP **SHALL NOT** make consent for the additional processing a condition of the identity service.	
The IdP **SHOULD** employ technical measures, such as the use of pairwise pseudonymous identifiers described in Sec. 6.2.5 or privacy-enhancing cryptographic protocols, to provide disassociability and discourage subscriber activity tracking and profiling between RPs.	IA-4(8) IA-8 (6)
An IdP **MAY** disclose information on subscriber activities to RPs for security purposes, such as communication of suspicious activity or a compromised subscriber account as described in Sec. 5.7, if stated within the trust agreement.	
An RP **MAY** disclose information on subscriber activities to IdPs for security purposes, such as communication of suspicious activity or a compromised RP subscriber account, if stated within the trust agreement.	
An IdP **SHOULD** signal subscriber account termination to RPs that have been provisioned with federated identifiers bound to that subscriber account using shared signaling as discussed in Sec. 5.7.	
RPs that receive such a signal from the IdP **SHALL** terminate the RP subscriber account and remove all personal information associated with the RP subscriber account, except what is required for audit and security purposes.	
The following requirements apply specifically to federal agencies: 1. The agency **SHALL** consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the requirements of the Privacy Act are triggered by the agency that is acting as an IdP, by the agency that is acting as an RP, or both (see Sec. 9.4).	
2. The agency **SHALL** publish or identify coverage by a System	

of Records Notice (SORN) as applicable.	
3. The agency **SHALL** consult with their SAOP to conduct an analysis determining whether the requirements of the E-Government Act are triggered by the agency that is acting as an IdP, the agency that is acting as an RP, or both.	
4. The agency **SHALL** publish or identify coverage by a Privacy Impact Assessment (PIA) as applicable.	
If the RP subscriber account lifecycle process gives the RP access to attributes through a provisioning API as discussed in Sec. 5.4.3, additional privacy measures **SHALL** be implemented given the wide nature of information access. Specifically, it is possible for the attributes of a subscriber to be provided to an RP without the subscriber ever interacting with the RP in question.	
As a consequence, when a provisioning API is used, the IdP **SHALL** minimize the attributes made available to the RP.	
To prevent the transmission of attributes for users that will never use an RP, the IdP **SHALL** limit the population of subscriber accounts available via the provisioning API to the population of subscribers authorized to use the RP by the trust agreement.	
5.6. Reauthentication and Session Requirements in Federated Environments	
Due to the distributed nature of a federated system, the subscriber's sessions with the IdP and with the RP terminate independently of each other. The RP **SHALL NOT** assume that the subscriber has an active session at the IdP past the issuance time of the assertion.	
The IdP **SHALL NOT** assume that termination of the subscriber's session at the IdP will propagate to any sessions that subscriber would have at downstream RPs.	
The RP and IdP **MAY** communicate session termination requests to other parties in the federation network, if supported by the federation protocol.	

At the time of a federated login request, the subscriber **MAY** have a pre-existing session at the IdP which **MAY** be used to generate an assertion to the RP.	
The IdP **SHALL** communicate any information it has regarding the time of the subscriber's latest authentication event at the IdP, and the RP **MAY** use this information in making authorization and access decisions.	
Depending on the capabilities of the federation protocol in use, the IdP **SHOULD** allow the RP to request that the subscriber repeat authentication at the IdP as part of a federation request.	
An RP requiring authentication through a federation protocol **SHALL** specify the maximum acceptable authentication age to the IdP, either through the federation protocol (if possible) or through the parameters of the trust agreement.	
The authentication age represents the time since the last authentication event in the subscriber's session at the IdP, and the IdP **SHALL** reauthenticate the subscriber if they have not been authenticated within that time period.	
The IdP **SHALL** communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for authentication at the RP and to determine the time for the next reauthentication event.	
If an RP is granted access to an identity API along with the assertion, the lifetime of the access to the identity API is independent from the lifetime of the assertion itself. Since access to the identity API is often combined with access to additional APIs, it is common for this access to be valid long after the assertion has expired and possibly after the session with the RP has ended, allowing the RP to access APIs on the subscriber's behalf while the subscriber is no longer present. As a consequence, the RP's ability to successfully fetch additional attributes through an identity API **SHALL NOT** be used to establish a session at the RP.	
Likewise, inability to access an identity API **SHOULD NOT** be used to end the session at the RP.	

5.7. Shared Signaling	
In some environments, it is useful for the IdP and RP to send information to each other outside of the federation transaction. These signals can communicate important changes in state between parties that would not be otherwise known. The use of any shared signaling **SHALL** be documented in the trust agreement between the IdP and RP.	
Signaling from the IdP to the RP **SHALL** require a static trust agreement.	
Signaling from the RP to the IdP **MAY** be used in a static or dynamic trust agreement.	
Any use of shared signaling **SHALL** be documented and made available to the authorized party stipulated by the trust agreement.	
This documentation **SHALL** include the events under which a signal is sent, the information included in such a signal (including any attribute information), and any additional parameters sent with the signal.	
The use of shared signaling **SHALL** be subject to privacy review under the trust agreement.	
The IdP **MAY** send a signal regarding the following changes to the subscriber account: ● The account has been terminated. ● The account is suspected of being compromised. ● Attributes of the account, including identifiers other than the federated identifier (such as email address or certificate CN), have changed. ● The possible range of IAL, AAL, or FAL for the account has changed.	
The RP **MAY** send a signal regarding the following changes to the RP subscriber account: ● The account has been terminated.	

● The account is suspected of being compromised. ● An RP-managed bound authenticator is added. ● An RP-managed bound authenticator is removed.	
Additional signals from both the IdP and RP **MAY** be allowed subject to privacy and security review as part of the trust agreement.	
6. Assertions	
Assertions **SHALL** represent a discrete authentication event of the subscriber at the IdP and **SHALL** be processed as a discrete authentication event at the RP.	
All assertions **SHALL** include the following attributes: 1. Subject identifier: An identifier for the party to which the assertion applies (i.e., the subscriber). 2. Issuer identifier: An identifier for the issuer of the assertion (i.e., the IdP). 3. Audience identifier: An identifier for the party intended to consume the assertion (i.e., the RP). 4. Issuance time: A timestamp indicating when the IdP issued the assertion.	IA-8
5. Validity time window: A period of time outside of which the assertion **SHALL NOT** be accepted as valid by the RP for the purposes of authenticating the subscriber and starting an authenticated session at the RP. This is usually communicated by means of an expiration timestamp for the assertion in addition to the issuance timestamp. 6. Assertion identifier: A value uniquely identifying this assertion, used to prevent attackers from replaying prior assertions. 7. Signature: Digital signature or message authentication code (MAC), including key identifier or public key associated with the IdP, covering the entire assertion. 8. Authentication time: A timestamp indicating when the IdP last verified the presence of the subscriber at the IdP through a primary authentication event (if available). 9. IAL: Indicator of the IAL of the subscriber account being represented in the assertion, or an indication that no IAL is asserted. 10. AAL: Indicator of the AAL used when the subscriber	

authenticated to the IdP, or an indication that no AAL is asserted. 11. FAL: An indicator of the IdP's intended FAL of the federation process represented by the assertion.	
If the assertion is used at FAL3 with a bound authenticator as described in Sec. 6.1.2, the assertion **SHALL** include the following: 1. Authenticator binding: The public key, key identifier, or other identifier of subscriber-held bound authenticator (for IdP-managed bound authenticators) or indicator that an RP-managed bound authenticator is required for verification of this assertion.	
Assertions **MAY** also include additional items, including the following information: 1. Attribute values and derived attribute values: Information about the subscriber. 2. Attribute metadata: Additional information about one or more subscriber attributes, such as those described in NIST Internal Report 8112 [NISTIR8112].	
Assertions **SHOULD** specify the AAL when an authentication event is being asserted and IAL when identity proofed attributes (or values derived from those attributes) are being asserted.	
All metadata within the assertion **SHALL** be validated by the RP upon receipt: ● *Issuer verification*: ensuring the assertion was issued by the IdP the RP expects it to be from. ● *Signature validation*: ensuring the signature of the assertion is valid and corresponds to a key belonging to the IdP sending the assertion. ● *Time validation*: ensuring the expiration and issue times are within acceptable limits of the current timestamp. ● *Audience restriction*: ensuring this RP is the intended recipient of the assertion.	
An RP **SHALL** treat subject identifiers as not inherently globally unique. Instead, the value of the assertion's subject identifier is usually in a namespace under the assertion issuer's control. This allows an RP to talk to multiple IdPs without incorrectly conflating	IA-8 IA-12 b.

subjects from different IdPs.	
Assertions **MAY** include additional attributes about the subscriber. Section 6.2.3 contains privacy requirements for presenting attributes in assertions.	
The RP **MAY** be given limited access to an identity API as discussed in Sec. 6.3 along with the assertion, which the RP can use to fetch additional identity attributes for the subscriber.	
The assertion's validity time window is the time between its issuance and its expiration. This window needs to be large enough to allow the RP to process the assertion and create a local application session for the subscriber, but should not be longer than necessary for such establishment. Long-lived assertions have a greater risk of being stolen or replayed; a short assertion validity time window mitigates this risk. Assertion validity time windows **SHALL NOT** be used to limit the session at the RP. See Sec. 5.3 for more information.	
6.1.1. Bearer Assertions	
Note that mere possession of a bearer assertion or reference is not always enough to impersonate a subscriber. For example, if an assertion is presented in the back-channel federation model (described in Sec. 7.1), additional controls **MAY** be placed on the transaction (such as identification of the RP and assertion injection protections) that help further protect the RP from fraudulent activity.	
6.1.2. Bound Authenticators	
A bound authenticator **SHALL** be unique per subscriber at the RP such that two subscribers cannot present the same authenticator for their separate RP subscriber accounts.	
All bound authenticators **SHALL** be phishing resistant. Consequently, subscriber-chosen values such as a memorized secret cannot be used as bound authenticators.	
The RP **SHALL** accept authentication from a bound authenticator only in the context of processing an assertion. Consequently, the	

subscriber can not use a bound authenticator to log into the RP directly, bypassing the IdP in the process	
6.1.2.1. IdP-Managed Bound Authenticators	
When the bound authenticator is managed by the IdP as in Fig. 9, a unique identifier for the authenticator (such as its public key) **SHALL** be included in the assertion presented to the RP.	
The RP **SHALL** prompt the subscriber to prove possession of the identified bound authenticator.	
An IdP-managed bound authenticator **MAY** be distinct from the primary authenticator the subscriber uses to authenticate to the IdP.	
Bound authenticators managed at the IdP **SHALL** be phishing resistant and **SHALL** be independently dereferenceable by the RP based on a mutually-trusted security framework, such as a public-key infrastructure.	
When processing an IdP-managed bound authenticator for the first time, the RP **SHOULD** verify whether the authenticator being presented is appropriate to be associated with the subscriber account, such as through account resolution from the attributes in the authenticator's presented information.	
6.1.2.2. RP-Managed Bound Authenticators	
When the bound authenticator is managed by the RP as in Fig. 10, the IdP **SHALL** include an indicator in the assertion that the assertion is to be used with a bound authenticator at FAL3.	
The unique identifier for the authenticator (such as its public key) **SHALL** be stored in the RP subscriber account.	
For RP-provided authenticators, the administrator of the RP **SHALL** issue the authenticator to the subscriber directly for use with an FAL3 login.	IA-5 (16)
The administrator of the RP **SHALL** store a unique identifier for the	

bound authenticator in the RP subscriber account.	
The administrator of the RP **SHALL** determine through independent means that the party to which the authenticator is issued is the identified subject of the RP subscriber account.	
For subscriber-provided authenticators, if no bound authenticators are associated with the RP subscriber account, the RP **SHALL** perform a binding ceremony to establish the connection between the authenticator, the subscriber, and the RP subscriber account as shown in Fig. 11.	
The RP **SHALL** first establish an authenticated session using federation with an assertion that meets all the other requirements of FAL3, including an indication that the assertion is intended for use at FAL3 with an RP-managed bound authenticator.	
The subscriber **SHALL** immediately be prompted to present and authenticate with the proposed authenticator.	
Upon successful presentation of the authenticator, the RP **SHALL** store a unique identifier for the authenticator (such as its public key) and associate this with the RP subscriber account associated with the federated identifier. If the subscriber fails to successfully present an appropriate authenticator, the binding ceremony fails.	
The binding ceremony session **SHALL** have a timeout of five minutes or less. The session used during the ceremony is not an authenticated session for the purposes of logging in.	
Upon successful completion of the binding ceremony, the RP **SHALL** immediately request a new assertion from the IdP at FAL3, including prompting the subscriber for the newly-bound authenticator.	
An RP **MAY** allow a subscriber to bind multiple subscriber-provided authenticators at FAL3. If this is the case, and the RP subscriber account has one or more existing bound authenticators, the binding ceremony makes use of the existing ability to reach FAL3.	
The subscriber **SHALL** first be prompted to present an existing	

bound authenticator to reach FAL3.	
Upon successful authentication, the RP **SHALL** immediately prompt the subscriber for the newly-bound authenticator.	
An RP **MAY** allow a subscriber to unbind a bound subscriber-provided authenticator from their RP subscriber account, thereby removing the ability to use that authenticator for FAL3.	
When a bound authenticator is unbound, the RP **SHALL** terminate all current FAL3 sessions for the subscriber and **SHALL** require reauthentication of the subscriber from the IdP. Note that in many cases, a subscriber will need to unbind a bound authenticator to account for a lost or compromised authenticator, and the subscriber will therefore not have access to the authenticator during the unbinding process.	
The RP **SHALL** notify the subscriber through an out-of-band mechanism, and **SHOULD** notify the IdP using a shared signaling system (see Sec. 5.7), if any of the following events occur: ● A new authenticator is bound to the RP subscriber account. ● An existing bound authenticator is unbound from the RP subscriber account.	
6.1.2.3. Processing Bound Authenticators	
The following requirements apply to all assertions associated with a bound authenticator: 1. The subscriber **SHALL** prove possession of the bound authenticator to the RP, in addition to presentation of the assertion itself.	
2. If the authenticator is managed at the IdP, reference to a given authenticator found within an assertion **SHALL** be trusted at the same level as all other information within the assertion.	
3. If the authenticator is managed at the IdP, the assertion **SHALL NOT** include an unencrypted private or symmetric key to be used as an authenticator with the presentation.	

4. The RP **SHALL** process and validate the assertion in addition to the bound authenticator.	
5. Failure to authenticate with the bound authenticator **SHALL** result in an error at the RP.	
6.2. Assertion Protection	
Independent of the binding mechanism (discussed in Sec. 6.1) or the federation model used to obtain them (described in Sec. 5.1), assertions **SHALL** include a set of protections to prevent attackers from manufacturing valid assertions or reusing captured assertions at disparate RPs. The protections required are dependent on the details of the use case being considered, and specific protections are listed here.	
6.2.1. Assertion Identifier	
Assertions **SHALL** be sufficiently unique to permit unique identification by the target RP.	
Assertions **MAY** accomplish this by use of an embedded nonce, issuance timestamp, assertion identifier, or a combination of these or other techniques.	
6.2.2. Signed Assertion	
Assertions **SHALL** be cryptographically signed by the issuer (IdP).	
The RP **SHALL** validate the digital signature or MAC of each such assertion based on the issuer's key.	
This signature **SHALL** cover the entire assertion, including its identifier, issuer, audience, subject, and expiration.	
The assertion signature **SHALL** either be a digital signature using asymmetric keys or a MAC using a symmetric key shared between the RP and issuer.	
Shared symmetric keys used for this purpose by the IdP **SHALL** be independent for each RP to which they send assertions, and are	

normally established during registration of the RP.	
Public keys for verifying digital signatures **SHALL** be transferred to the RP in a secure manner, and **MAY** be fetched by the RP in a secure fashion at runtime, such as through an HTTPS URL hosted by the IdP.	
Approved cryptography **SHALL** be used.	
6.2.3. Encrypted Assertion	
When encrypting assertions, the IdP **SHALL** encrypt the contents of the assertion using either the RP's public key or a shared symmetric key.	
Shared symmetric keys used for this purpose by the IdP **SHALL** be independent for each RP to which they send assertions, and are normally established during registration of the RP.	
Public keys for encryption **SHALL** be securely transferred to the IdP and **MAY** be fetched by the IdP in a secure fashion at runtime, such as through an HTTPS URL hosted by the RP.	
All encryption of assertions **SHALL** use approved cryptography.	
When personally-identifiable information is included in the assertion and the assertion is handled by intermediaries such as a browser, the federation protocol **SHALL** encrypt assertions to protect the sensitive information in the assertion from leaking to unintended parties. For example, a SAML assertion can be encrypted using XML-Encryption, or an OpenID Connect ID Token can be encrypted using JSON Web Encryption (JWE).	IA-8 (4)
6.2.4. Audience Restriction	
Assertions **SHALL** use audience restriction techniques to allow an RP to recognize whether or not it is the intended target of an issued assertion..	
All RPs **SHALL** check that the audience of an assertion contains an identifier for their RP to prevent the injection and replay of an	

assertion generated for one RP at another RP	
6.2.5. Pairwise Pseudonymous Identifiers	
6.2.5.1. General Requirements	
When using pairwise pseudonymous identifiers within the assertions generated by the IdP for the RP, the IdP **SHALL** generate a different federated identifier for each RP as described in Sec. 6.2.5.2 below. When PPIs are used with RPs alongside attributes, it may still be possible for multiple colluding RPs to re-identify a subscriber by correlation across systems using these identity attributes. For example, if two independent RPs each see the same subscriber identified with different pairwise pseudonymous identifiers, they could still determine that the subscriber is the same person by comparing the name, email address, physical address, or other identifying attributes carried alongside the pairwise pseudonymous identifier in the respective assertions.	IA-4(8) IA-8 IA-8 (6) IA-12 b.
Privacy policies **SHOULD** prohibit such correlation, and pairwise pseudonymous identifiers can increase effectiveness of these policies by increasing the administrative effort in managing the attribute correlation.	IA-4(8) IA-8 (6)
The proxy **SHALL NOT** disclose the mapping between the pairwise pseudonymous identifier and any other identifiers to a third party or use the information for any purpose other than federated authentication, related fraud mitigation, to comply with law or legal process, or in the case of a specific user request for the information.	IA-4(8) IA-8 (6)
6.2.5.2. Pairwise Pseudonymous Identifier Generation	
Pairwise pseudonymous identifiers **SHALL** contain no identifying information about the subscriber.	IA-4(8) IA-8 (6)
They **SHALL** also be unguessable by a party having access to some information identifying the subscriber.	IA-4(8) IA-8 (6)
Pairwise pseudonymous identifiers **MAY** be generated randomly and assigned to subscribers by the IdP or **MAY** be derived from	IA-4(8) IA-8 (6)

other subscriber information if the derivation is done in an irreversible, unguessable manner (e.g., using a keyed hash function with a secret key).	
Normally, the identifiers **SHALL** only be known by and used by one pair of endpoints (e.g., IdP-RP).	IA-4(8) IA-8 (6)
An IdP **MAY** generate the same identifier for a subscriber at multiple RPs at the request of those RPs, provided: ● The trust agreement stipulates a shared pseudonymous identifier for a specific family of RPs; ● The authorized party consents to and is notified of the use of a shared pseudonymous identifier; ● Those RPs have a demonstrable relationship that justifies an operational need for the correlation, such as a shared security domain or shared legal ownership; and ● All RPs sharing an identifier consent to being correlated in such a manner (i.e., one RP cannot request to have another RP's PPI without that other RP's knowledge and consent).	IA-4(8) IA-8 (6)
The RPs **SHALL** conduct a privacy risk assessment to consider the privacy risks associated with requesting a common identifier. See Sec. 9.2 for further privacy considerations.	IA-4(8) IA-8 (6)
The IdP **SHALL** ensure that only intended RPs are correlated; otherwise, a rogue RP could learn of the pseudonymous identifier for a set of correlated RPs by fraudulently posing as part of that set.	IA-4(8) IA-8 (6)
6.3. Identity APIs	
Attributes about the subscriber, including profile information, **MAY** be provided to the RP through a protected *attribute API* known as the *identity API*. The RP is granted limited access to the identity API during the federation transaction, in concert with the assertion.	
Access to the identity API **SHALL** be time limited. The time limitation is separate from the validity time window of the assertion and the lifetime of the authenticated session at the RP.	

Access to an identity API by the RP without an associated valid assertion **SHALL NOT** be sufficient for the establishment of an authenticated session at the RP.	
A given identity API deployment is expected to be capable of providing attributes for all subscribers for whom the IdP can create assertions. However, when access to the identity API is granted within the context of a federation transaction, the attributes provided by an identity API **SHALL** be associated with only the single subscriber identified in the associated assertion.	
If the identity API is hosted by the IdP, the returned attributes **SHALL** include the subject identifier for the subscriber. This allows the RP to positively correlate the assertion's subject to the returned attributes. Note that when access to an attribute API is provided as part of pre-provisioning of RP subscriber accounts as discussed in Sec. 5.4.1, the RP is usually granted blanket access to the identity API outside the context of the federated transaction and these requirements do not apply.	
6.3.1. Attribute Providers	
The attributes returned by the attribute provider are assumed to be independent of those returned directly from the IdP, and as such **MAY** use different identifiers, formats, or schemas.	IA-4(9)
The RP **SHALL** verify that the identified attribute provider is capable of providing the kinds of attributes that are present, under the auspices of the applicable trust agreement.	IA-4(9)
7. Assertion Presentation	
There are tradeoffs with each model, but each requires the proper validation of the assertion. Assertions **MAY** also be proxied to facilitate federation between IdPs and RPs using different presentation methods, as discussed in detail in Sec. 5.1.3.	
7.1. Back-Channel Presentation	
In the *back-channel* presentation model, the subscriber is given an	

assertion reference to present to the RP, generally through the front channel. The assertion reference itself contains no information about the subscriber and **SHALL** be resistant to tampering and fabrication by an attacker. The RP presents the assertion reference to the IdP, usually along with authentication of the RP itself, to fetch the assertion.	
The assertion reference: 1. **SHALL** be limited to use by a single RP.	
2. **SHALL** be single-use.	
3. **SHALL** be time limited, and **SHOULD** have a lifetime of no more than a small number of minutes in length.	
4. **SHALL** be presented along with authentication of the RP to the IdP.	
5. **SHALL** contain at least 128 bits of entropy	
The RP **SHALL** protect itself against injection of manufactured or captured assertion references by use of cross-site scripting protection or other accepted techniques.	
Conveyance of the assertion reference from the IdP to the subscriber, as well as from the subscriber to the RP, **SHALL** be made over an authenticated protected channel.	
Conveyance of the assertion reference from the RP to the IdP, as well as the assertion from the IdP to the RP, **SHALL** be made over an authenticated protected channel..	
When assertion references are presented, the IdP **SHALL** verify that the party presenting the assertion reference is the same party that requested the authentication. The IdP can do this by requiring the RP to authenticate itself when presenting the assertion reference to the IdP or through other similar means (see [RFC7636] for one protocol's method of dynamic RP verification)	

7.2. Front-Channel Presentation	
The RP **SHALL** protect itself against injection of manufactured or captured assertions by use of cross-site scripting protection and other accepted techniques.	
Conveyance of the assertion from the IdP to the subscriber, as well as from the subscriber to the RP, **SHALL** be made over an authenticated protected channel.	
7.3. Protecting Information	
Communications between the IdP and the RP **SHALL** be protected in transit using an authenticated protected channel.	
Communications between the subscriber and either the IdP or the RP (usually through a browser) **SHALL** be made using an authenticated protected channel.	
Additional attributes about the user **MAY** be included outside of the assertion itself by use of authorized access to an identity API as discussed in Sec. 6.3. Splitting user information in this manner can aid in protecting user privacy and allow for limited disclosure of identifying attributes on top of the essential information in the authentication assertion itself.	
The RP **SHALL**, where feasible, request derived attribute values rather than full attribute values as described in Sec. 9.3.	
The IdP **SHALL** support derived attribute values to the extent possible.	
8. Security (Informative)	
8.1. Federation Threats (Informative)	
8.2. Federation Threat Mitigation Strategies (Informative)	
9. Privacy Considerations (Informative)	
9.1. Minimizing Tracking and Profiling (Informative)	
9.2. Notice and Consent (Informative)	

References

SP 800-53	NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, Dec 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
SP 800-63	NIST Special Publication 800-63 Digital Identity Guidelines https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines