Special Publication 800-63C Conformance Criteria

Introduction

This document presents conformance criteria for NIST Special Publication 800-63C *Federation and Assertions*. This set of conformance criteria presents all normative requirements and controls for SP 800-63C for assurance levels FAL1, FAL2, and FAL3.

The conformance criteria are enumerated to facilitate referencing and indexing. Similar to the indexing of the inventory of controls for NIST Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*, the enumeration of the conformance criteria is separated into sections for criteria that apply to specific functional areas in SP 800-63C; this also is intended to facilitate referencing and indexing. An index is also provided for the complete set of conformance criteria to facilitate reference to specific topics and criteria.

All the conformance criteria are presented in the following format:

- **Requirement –** presentation of the normative requirement/control statement from SP 800-C.
- **Supplemental guidance** – presentation of informative guidance to facilitate the understanding, implementation and assessment for each criterion.
- **Assessment objective** – Presentation of the intended objective and outcome from the assessment of conformance for each criterion.
- **Potential assessment methods and objects** – Presentation of suggested methodologies for performing conformance assessment for each criterion.
- **Potential test methods** – Where applicable, presentation of suggested test methodologies for performing conformance testing for applicable criteria.

The only part of the conformance criteria that is normative is the normative requirement/control statement from SP 800-63C; all other parts and text of the criteria are informative. The supplemental guidance is intended to provide information to clarify the normative requirement/control and provide information about how to meet conformance for purposes of implementation and assessment. The assessment objective is intended to present the requirements and controls in terms of outcomes. SP 800-63-3 applies the NIST Risk Management Framework to identity systems and operations. The risk management framework advances the principle that organizations should have the flexibility to apply and tailor controls and requirements to best meet the risk environment of the organization, its systems and operations, target populations and use cases. Therefore, the conformance criteria are not intended to be prescriptive; rather, the criteria are intended to present the intended outcomes for the requirements and controls and allow flexibility in both the implementation and assessment of the criteria. Potential assessment and test methods are presented as suggested means to achieve/assess conformance to the requirement but should be considered suggestions rather than prescribed methods. Assessors have flexibility and responsibility to determine the most appropriate conformance assessment methods for the specific organization, system and operations, and risk environment.

While NIST Special Publications and guidance materials such as these conformance criteria are intended for federal agencies, the potential audiences and uses for the conformance criteria include:

- Federal agencies for the implementation of SP 800-63-3 and assessment of implementation, risks, and controls in meeting Federal Information Security Modernization Act (FISMA) requirements and responsibilities
- Credential Service providers for the implementation of services and products to meet conformance requirements of SP 800-63-3
- Organizations and services that perform assessment and, potentially, certification of conformance with SP 800-63-3 requirements
- Audit organizations that offer and provide audit services for determining federal agency or external non-federal service provider conformance to SP 800-63-3 requirements and controls
- The General Services Administration to facilitate activities to address the responsibility in Office of Management and Budget Policy Memo M-19-17: "*Determine the feasibility, in coordination with OMB, of establishing or leveraging a public or private sector capability for accrediting ICAM products and services available on GSA acquisition vehicles, and confirm the capability leverages NIST developed criteria for 800-63 assurance levels. This capability should support and not duplicate existing Federal approval processes*."

These conformance criteria are publicly available at the NIST Identity and Access Management Resource Center: https://www.nist.gov/topics/identity-access-management. NIST anticipates that this resource may be periodically updated based on federal agency and industry experience and feedback. Questions and comments on these resources may be sent to dig-comments@nist.gov.

Digital Identity Model Roles

SP 800-63C Figure 5-1 presents the model for *Federation* and describes the various entities and interactions that comprise the model as illustrated below.

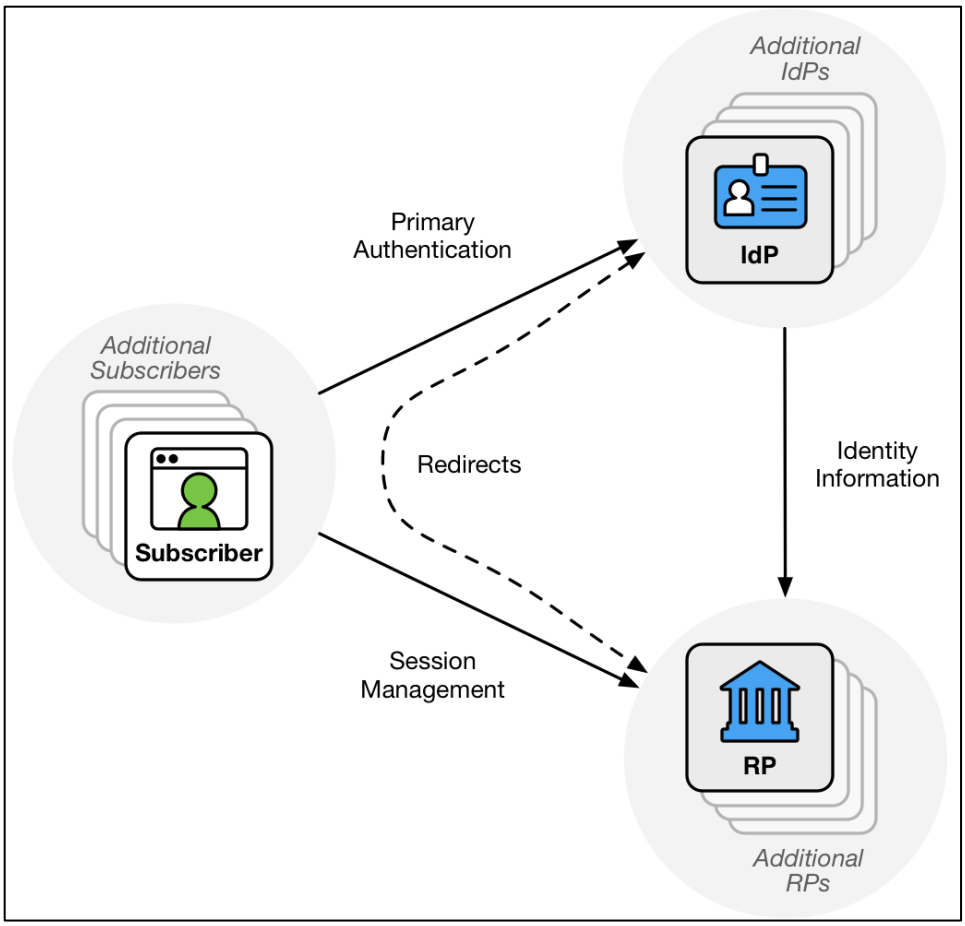

Figure 5-1 Federation

SP 800-63A presents requirements, controls, and activities to perform the identity proofing and enrollment of the subscriber depicted on the left side of Figure 5-1 *Federation.* SP 800-63B presents requirements, controls, and activities of authenticators used for Primary Authentication shown at the top of the diagram. SP 800-63B also presents requirements, controls, and activities of session management shown at the bottom of the diagram.

SP 800-63C presents requirements, controls, and activities to perform federated identity transactions as depicted in Figure 5-1 *Federation*. The subscriber authenticates to the Identity Provider (IdP) using their credential. The IdP then passes identity information about the subscriber in the form of an assertion to the Relying Party (RP). After the RP processes the assertion, the subscriber is then logged in to the RP. The RP then manages the subscriber's session over time.

The role of the IdP is distinct from the Credential Service Provider (CSP), though they are often fulfilled by the same entity. The IdP provides federation-specific services, and the CSP provides the account and credential services the IdP uses for authentication. The RP could be a separate entity in a separate organization, or it could be another service within the IdP's own organization. In either case, the IdP and RP have a trust relationship with each other that is the anchor of the federation process. The SP 800-63C Conformance Criteria are applicable to the

roles of IdP and RP, as well as to any other entities involved such as a federation authority or proxy, as applicable.

Note that in the federation model, the RP does not see the credential directly, but the IdP does. Therefore, the role of Verifier as described in SP 800-63B is fulfilled by the IdP in the federation model and the SP 800-63B Conformance Criteria are applicable to the IdP in its handling of authenticators.

Digital identity service providers outside the federal government that voluntarily adopt SP 800-63-3 as a standard will need to examine the roles performed for digital authentication to determine the applicability of the SP 800-63C Conformance Criteria to their specific implementation.

Conditional Requirements

Some requirements in SP 800-63C are conditional based on circumstances. These requirements are characterized as follows; IF (a conditional circumstance occurs), THEN this requirement(s) shall apply. Conditional Conformance Criteria follow the same pattern in the statement of the normative requirement: IF (this conditional circumstance occurs). THEN the normative requirement and conformance criterion shall apply. Conditional conformance criteria are presented in the same format as all other criteria. Assessors will need to determine whether the conditional circumstance occurs for a specific implementation in order to determine the applicability of the conditional conformance criterion to that implementation.

Federal Agency Unique Requirements

Some requirements in SP 800-63C apply uniquely to federal agencies and the conformance criteria for these requirements clearly indicate this status. In general, these conformance criteria do not apply to entities external to the federal government that have voluntarily chosen to adopt the SP 800-63C standard or are otherwise applying the conformance criteria to the services that they provide.

Organization of criteria

The conformance criteria presented below are organized into categories roughly as SP 800-63C is organized. Not all categories will need to be evaluated in all situations. The categories are as follows:

Category	Applicability
ASSN	Assertions across all FALs
ATTR	Attributes carried within an assertion
ID	Identifiers for subscribers asserted by IdPs
IDP	Identity Providers (general requirements)
TRUST	All IdPs and RPs in trust agreements and trust frameworks
FED	Federation authorities
BACK	IdPs and RPs using back-channel presentation mechanisms
FRONT	IdPs and RPs using front-channel presentation mechanisms

CRYPTO	Cryptographic methods and keys used by IdPs and RPs to protect assertions and transactions
SIG	IdPs signing assertions and RPs validating assertion signatures (at all FALs)
FAL2	IdPs and RPs operating at FAL2 (or above)
FAL3	IdPs and RPs operating at FAL3
PROXY	Identity proxies
ALLOW	IdPs and RPs using lists of pre-approved parties and circumstances (also known as an "allowlist" or, formerly, a "whitelist")
RUNTM	IdPs and RPs using decisions made at runtime by an authorized party
SESS	IdPs and RPs using session management

Index to Assertion Criteria

There are 10 requirements that apply to assertions across all FALs.

ID	63C Section		ID	63C Section
ASSN-1	4		ASSN-6	6.2
ASSN-2	4		ASSN-7	6.2.4
ASSN-3	4		ASSN-8	6.2.4
ASSN-4	6		ASSN-9	7.1
ASSN-5	6		ASSN-10	7.2

Index to Assertion Attribute Criteria

There are 7 requirements that apply to attributes carried within an assertion.

ID	63C Section		ID	63C Section
ATTR-1	4.2		ATTR-5	7
ATTR-2	5.3		ATTR-6	7.3
ATTR-3	6		ATTR-7	7.3
ATTR-4	7			

Index to Identifier Criteria

There are 7 requirements that apply to identifiers for subscribers asserted by IdPs.

ID	63C Section		ID	63C Section
ID-1	6		ID-5	6.3.2
ID-2	6.3.1		ID-6	6.3.2
ID-3	6.3.2		ID-7	6.3.2
ID-4	6.3.2			

Index to IdP Criteria

There are 6 requirements that apply to all identity providers.

ID	63C Section		ID	63C Section
IDP-1	4.1		IDP-4	4.2
IDP-2	4.2		IDP-5	5.1.2
IDP-3	4.2		IDP-6	5.2

Index to Trust Relationship Criteria

There are 9 requirements that apply to all IdPs and RPs in trust agreements and trust frameworks.

ID	63C Section		ID	63C Section
TRUST-1	4.2		TRUST-6	5.2
TRUST-2	4.2		TRUST-7	5.2
TRUST-3	4.2		TRUST-8	5.2
TRUST-4	5.1.1		TRUST-9	5.2
TRUST-5	5.2			

Index to Federation Authority Criteria

There are 5 requirements that apply to federation authorities.

ID	63C Section		ID	63C Section
FED-1	5.1.3		FED-4	5.1.3
FED-2	5.1.3		FED-5	5.1.3
FED-3	5.1.3			

Index to Back-Channel Criteria

There are 8 requirements that apply to IdPs and RPs using back-channel presentation mechanisms.

ID	63C Section		ID	63C Section
BACK-1	6.2.3		BACK-5	7.1
BACK-2	7.1		BACK-6	7.1
BACK-3	7.1		BACK-7	7.1
BACK-4	7.1		BACK-8	7.1

Index to Front-Channel Criteria

There are 4 requirements that apply to IdPs and RPs using front-channel presentation mechanisms.

ID	63C Section		ID	63C Section

FRONT-1	4		FRONT-3	7.3
FRONT-2	7.2		FRONT-4	7.3

Index to Cryptographic Method and Key Material Criteria

There are 8 requirements that apply to cryptographic methods and keys used by IdPs and RPs to protect assertions and transactions.

ID	63C Section		ID	63C Section
CRYPTO-1	4		CRYPTO-5	5.1.2
CRYPTO-2	4.1		CRYPTO-6	5.1.2
CRYPTO-3	5.1.1		CRYPTO-7	6.2.2
CRYPTO-4	5.1.1		CRYPTO-8	6.2.2

Index to Assertion Signature Criteria

There are 5 requirements that apply to IdPs signing assertions and RPs validating assertion signatures (at all FALs).

ID	63C Section		ID	63C Section
SIG-1	4.1		SIG-4	6.2.2
SIG-2	6.2.2		SIG-5	6.2.2
SIG-3	6.2.2			

Index to FAL2 Criteria

There are 4 requirements that apply to IdPs and RPs operating at FAL2 (or above) with encrypted assertions.

ID	63C Section		ID	63C Section
FAL2-1	6.2.3		FAL2-3	6.2.3
FAL2-2	6.2.3		FAL2-4	6.2.3

Index to FAL3 Criteria

There are 4 requirements that apply to IdPs and RPs operating at FAL3 with holder-of-key assertions.

ID	63C Section		ID	63C Section
FAL3-1	6.1.2		FAL3-3	6.1.2
FAL3-2	6.1.2		FAL3-4	6.1.2

Index to Proxy Criteria

There are 3 requirements that apply to identity proxies.

ID	63C Section		ID	63C Section
PROXY-1	4		PROXY-3	6.3.1
PROXY-2	5.1.4			

Index to Allowlist Criteria

There are 3 requirements that apply to IdPs and RPs using lists of pre-approved parties and circumstances (also known as an "allowlist" or, formerly, a "whitelist").

ID	63C Section		ID	63C Section
ALLOW-1	4.2		ALLOW-3	4.2
ALLOW-2	4.2			

Index to Runtime Decision Criteria

There are 7 requirements that apply to IdPs and RPs using decisions made at runtime by an authorized party.

ID	63C Section		ID	63C Section
RUNTM-1	4.2		RUNTM-5	4.2
RUNTM-2	4.2		RUNTM-6	5.1.1
RUNTM-3	4.2		RUNTM-7	5.1.2
RUNTM-4	4.2			

Index to Session Management Criteria

There are 5 requirements that apply to IdPs and RPs using session management.

ID	63C Section		ID	63C Section
SESS-1	5.3		SESS-4	6
SESS-2	5.3		SESS-5	6
SESS-3	6			

1 Assertion Conformance Criteria

All IdPs generating assertions and RPs consuming assertions SHALL be assessed on the following criteria:

ASSN-1	**REQUIREMENT**: All assertions SHALL be used with a federation protocol as described in Section 4. (4) **SUPPLEMENTAL GUIDANCE**: Assertions are cryptographically protected statements about a subject, and they are a core component of federation systems. Assertions could be generated, carried, and stored for a variety of reasons outside of their use in a federation protocol. While these are valid uses, federation protocols provide additional constraints and boundaries that make assertions trustable for login purposes, including how the assertion is presented and under what circumstances it is generated. The requirements in this document apply only to assertions as used within federation protocols, assertions being tested are used within a federation protocol to ensure that assertions accepted for login and access are intended to be used in that manner. Any assertions generated in the system for any other purposes (such as audit records or API access) should not be able to be confused for a login assertion by any party. Details of federation protocol models, and the trust contexts that drive them, are presented in section 4. **ASSESSMENT OBJECTIVE:** Determine whether assertions used for authentication purposes are presented only within a federation protocol and not through some other mechanism. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The generation of assertions by the IdP and the RP's login process to ensure that assertions are carried through a federation protocol.

ASSN-2	**REQUIREMENT**: All assertions SHALL comply with the detailed requirements in Section 6. (4) **SUPPLEMENTAL GUIDANCE**: All federation assertions must meet all of the requirements referenced in these conformance criteria regardless of FAL. See the details of these requirements in [ASSN-5], [ASSN-6], [ASSN-7], [ASSN-8], and the requirements of [ASSN-9] and [ASSN-10] as applicable. **ASSESSMENT OBJECTIVE:** Determine whether assertions used for login meet all relevant requirements. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Assertions generated by the IdP and accepted by the RP against all specific requirements.

	Test: The rejection of assertions that do not meet one or more of the requirements.

ASSN-3	**REQUIREMENT**: All assertions SHALL be presented using one of the methods described in Section 7. (4) **SUPPLEMENTAL GUIDANCE**: Assertions created during a federation transaction need to be presented to the RP, and the method of presentation affects the security aspects and requirements of the assertion itself. These guidelines specify two possible methods of presentation (front-channel and back-channel), and only one of these can be used to present any given assertion. **ASSESSMENT OBJECTIVE:** Determine whether the presentation method used by the IdP and RP fits one of the defined presentation methods, either front-channel or back-channel. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The method used to present the assertion to the RP and look for either: the presentation of an assertion reference which is then traded for an assertion (back-channel), or the presentation of an assertion carried directly by the subscriber's device (front-channel).

ASSN-4	**REQUIREMENT**: Assertions SHOULD specify the AAL when an authentication event is being asserted and IAL when identity proofed attributes (or references based thereon) are being asserted. If not specified, the RP SHALL NOT assign any specific IAL or AAL to the assertion. (6) **SUPPLEMENTAL GUIDANCE**: Any given IdP could support accounts at multiple IALs, and each account could support multiple authenticators with different AALs. Unless an RP is specifically told what IAL and AAL a given assertion represents, regardless of which IdP the assertion comes from or which subscriber is identified, the RP may not assign or assume any specific IAL or AAL for the assertion. Even the lowest levels of IAL1 and AAL1 have requirements associated with them that might not have been fulfilled for a specific request. If the RP does not modify its process based on IAL or AAL, this requirement does not apply. **ASSESSMENT OBJECTIVE**: Confirm the RP's policies for processing logins do not assign a default IAL and AAL if levels are not specified in the assertion. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The code, configuration, and policies of the RP to examine its processing of assertions that lack IAL and AAL information. **Test**: Generate an assertion for an RP that does not include any IAL or AAL information, examine the RP's processing behavior. Generate another assertion

	for the RP that includes a minimum IAL or AAL and document changes in an RP's behavior.

ASSN-5	*If the federation protocol includes an identity API for fetching attributes:* **REQUIREMENT**: The ability to successfully fetch such additional attributes SHALL NOT be treated as equivalent to processing the assertion. (6) **SUPPLEMENTAL GUIDANCE**: Only the processing of a valid assertion should be used to create an authenticated session at an RP. Some identity protocols allow the RP to fetch additional attribute information from an identity API using an "authorization component" that is issued alongside the assertion. However, while an assertion is a time-bound statement of the subscriber's presence, these authorization components, such as the OAuth access token issued in OpenID Connect, are often designed to continue to function long after the subscriber is departed. These components are often also usable with additional APIs and can sometimes even be issued to an RP when the subscriber is not present. Therefore, the use of an authorization component to fetch subscriber information is not a reliable indicator for the subscriber's presence in the same way that an assertion is. If the RP does not use any attribute fetching API, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Confirm that access to identity APIs is not sufficient to create or set an authorized state at the RP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Give an RP access to an identity API separate from an assertion and ensure that the RP does not log in the subscriber as a result. Ensure that an RP does not call the identity API as a means of determining if a subscriber is still present or logged in.

ASSN-6	**REQUIREMENT**: Independent of the binding mechanism (discussed in Section 6.1) or the federation model used to obtain them (described in Section 5.1), assertions SHALL include a set of protections to prevent attackers from manufacturing valid assertions or reusing captured assertions at disparate RPs. (6.2) **SUPPLEMENTAL GUIDANCE**: Assertions are the fundamental building block of a federated identity transaction, and protecting assertions is essential to the security of the overall system. If an attacker were able to create or modify an assertion and have that assertion accepted by an RP, the attacker would be able to impersonate a valid subscriber and log in to the target system. If an attacker were able to capture an assertion in transit and replay that assertion to a different RP, the attacker would be able to steal a valid session from the legitimate subscriber and log in to the target system. As a consequence, there are a suite of protections that are required for all assertions in a federated system, regardless of how the trust between the parties is established or how the assertion itself is

	delivered. An assertion has to use all of the protection mechanisms listed in order to be considered compliant. **ASSESSMENT OBJECTIVE:** Determine whether the assertions generated by the IdP and accepted by the RP use all of the protection mechanisms listed individually in this section. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Assertions generated by the IdP and accepted by the RP to determine they meet all requirements.

ASSN-7	**REQUIREMENT**: Assertions SHALL use audience restriction techniques to allow an RP to recognize whether or not it is the intended target of an issued assertion. (6.2.4) **SUPPLEMENTAL GUIDANCE**: Assertions are targeted messages from an IdP to an RP that are designed to be created in direct response to a specific federated login process. Each assertion needs to be targeted to specific RPs so that an assertion intended for one RP cannot be used at an unintended RP, either by the subscriber or an attacker. An assertion is allowed to have multiple target RPs, and it must have at least one. **ASSESSMENT OBJECTIVE:** Determine whether all assertions include audience restrictions identifying the target RP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate to an IdP to log in to an RP and examine the generated assertion to ensure that it includes audience restrictions that identify the RP.

ASSN-8	**REQUIREMENT**: 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. (6.2.4) **SUPPLEMENTAL GUIDANCE**: RPs have to check that assertions they receive are in fact targeted toward them and not a different RP. The RP needs to know what audience identifier the IdP uses to refer to the RP and the RP needs to ensure that that identifier is included in the audience target section of the assertion. An RP has to reject any assertion that the RP is not the intended audience for. Since an assertion can have multiple target RPs, an RP might need to check that its identifier is included in a structure instead of checking against a single value. **ASSESSMENT OBJECTIVE:** Determine whether RPs enforce audience restrictions in presented assertions. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**:

	Test: Log in to an RP with an assertion with a valid audience restriction field to ensure the RP accepts the assertion. Present the RP with an assertion that does not include the RP in its audience restriction field (or omits the audience restriction field) but is otherwise valid and ensure the RP rejects the assertion.

ASSN-9	*If using the back-channel presentation model:* **REQUIREMENT**: Elements within the assertion SHALL be validated by the RP, including: • 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 corresponds to the key related 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. (7.1) **SUPPLEMENTAL GUIDANCE**: [Same as ASSN-10] It is not sufficient for an assertion to be delivered to the RP with the subscriber's identity and authentication information, the RP has to validate all parts of the assertion as enumerated here to ensure the assertion is in fact valid and correct. These requirements stand regardless of how the assertion is delivered to the RP. **ASSESSMENT OBJECTIVE:** Determine whether the RP validates all required components of the assertion. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Deliver fraudulent assertions to the RP that separately invalidate each of the requirements above and ensure that the RP rejects each, such as: • An assertion with an incorrect, missing, or invalid issuer • An assertion with an incorrect, missing, or invalid signature • An assertion that has expired before the RP processes it • An assertion that claims to have been issued in the future • An assertion that does not include the RP as an intended audience

ASSN-10	*If using the front-channel presentation model:* **REQUIREMENT**: Elements within the assertion SHALL be validated by the RP including: • Issuer verification: ensuring the assertion was issued by the expected IdP. • Signature validation: ensuring the signature of the assertion corresponds to the key related to the IdP making 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. (7.2) **SUPPLEMENTAL GUIDANCE**: [Same as ASSN-9] It is not sufficient for an assertion to be delivered to the RP with the subscriber's identity and authentication information, the RP has to validate all parts of the assertion as enumerated here to ensure the assertion is in fact valid and correct. These requirements stand regardless of how the assertion is delivered to the RP. **ASSESSMENT OBJECTIVE:** Determine whether the RP validates all required components of the assertion. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Deliver fraudulent assertions to the RP that separately invalidate each of the requirements above and ensure that the RP rejects each, such as: • An assertion with an incorrect, missing, or invalid issuer • An assertion with an incorrect, missing, or invalid signature • An assertion that has expired before the RP processes it • An assertion that claims to have been issued in the future • An assertion that does not include the RP as an intended audience

2 Assertion Attribute Conformance Criteria

All IdPs generating assertions containing attributes and RPs consuming assertions containing attributes SHALL be assessed on the following criteria:

ATTR-1	*If the federation protocol in use allows for optional attributes:* **REQUIREMENT**: The subscriber SHALL be given the option to decide whether to transmit those attributes to the RP. An IdP MAY employ mechanisms to remember and re-transmit the exact attribute bundle to the same RP. (4.2) **SUPPLEMENTAL GUIDANCE**: Some federation protocols allow for attributes to be requested for optional release. In such cases, the IdP needs to provide the subscriber the opportunity during the process to decide whether to transmit those optional attributes to the RP. Optional attributes and the method of selection need to be clearly delineated for subscribers. If the federation protocol does not support optional attributes in the request, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether the subscriber can selectively approve or deny the RP access to any optional attributes. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: RP list of required and optional attributes, if any; the UI/UX that show the points and messaging in the user flow where optional attributes are delineated for subscriber selection. **Test**: Observe a subscriber log in and trigger a runtime decision that includes a request for optional attributes. Observe that the subscriber is prompted with a request for release of those attributes. Have the subscriber deny those optional attributes to the RP and ensure that they are not released to the RP in that transaction.

ATTR-2	**REQUIREMENT**: The IdP SHALL communicate any information it has regarding the time of the latest authentication event at the IdP, and the RP MAY use this information in determining its access policies. (5.3) **SUPPLEMENTAL GUIDANCE**: A federated assertion is generated in the context of an active authentication event for the subscriber at the IdP. When communicating the authentication state of the subscriber to the RP in an assertion, the IdP has to communicate the timing of that authentication event to the RP. This information can help the RP make access decisions, such as requesting the subscriber to re-authenticate at the IdP directly before being allowed to access highly sensitive information.

	ASSESSMENT OBJECTIVE: Determine whether assertions generated by the IdP include a timestamp of the authentication event. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Assertions from the IdP to ensure the authentication timestamp is included. **Test**: Authenticate to an IdP to log in to an RP and examine that the authentication timestamp is included in the assertion. Re-authenticate to the IdP to set a new authentication time. Create a new login from the IdP to an RP and ensure the new assertion contains the new authentication timestamp.

ATTR-3	**REQUIREMENT**: All assertions SHALL include the following assertion metadata: • Subject: An identifier for the party that the assertion is about (i.e., the subscriber). • Issuer: An identifier for the IdP that issued the assertion. • Audience: An identifier for the party intended to consume the assertion (i.e., the RP). • Issuance: A timestamp indicating when the IdP issued the assertion. • Expiration: A timestamp indicating when the assertion expires and SHALL no longer be accepted as valid by the RP (i.e., the expiration of the assertion and not the expiration of the session at the RP). • Identifier: A value uniquely identifying this assertion, used to prevent attackers from replaying prior assertions. • Signature: Digital signature or message authentication code (MAC), including key identifier or public key associated with the IdP, for the entire assertion. • 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). (6) **SUPPLEMENTAL GUIDANCE**: This criterion presents all of the elements required in every assertion. Each element provides a different and vital piece of information for the secure conveyance of the identity information. Assertions can contain additional information, whether about the subscriber or about the authentication event itself, but these fields are all required at all FALs. **ASSESSMENT OBJECTIVE:** Determine whether assertions generated contain at least this list of required fields with appropriate values and that the assertion's contents are covered by the signature. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Authenticate to an IdP to log in to an RP to generate an assertion, examine the assertion for all listed fields and their contents.

ATTR-4	**REQUIREMENT**: The IdP SHALL transmit only those attributes that were explicitly requested by the RP. (7) **SUPPLEMENTAL GUIDANCE**: IdPs usually have access to many different attributes for each subscriber. In the scope of a single federated login request, only those attributes that were explicitly requested by the RP are to be transmitted by the IdP. This request can be communicated at runtime, such as with OpenID Connect's scope and claims parameters, or it can be configured ahead of time for a given RP. **ASSESSMENT OBJECTIVE:** Determine whether all attributes transmitted by the IdP were explicitly requested by the RP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The configuration of the IdP and a statement of practices on attribute release. If available (such as with a static RP configuration), compare the list of attributes transmitted by the IdP and the list of attributes requested by the RP. **Test**: Log in to an RP and ensure that no attributes exist in the assertion that were not requested by the RP. If the federation protocol allows variability of the requested parameters at runtime, have the RP request different sets of attributes across multiple logins to ensure that only requested attributes are released.

ATTR-5	**REQUIREMENT**: RPs SHALL conduct a privacy risk assessment when determining which attributes to request. (7) **SUPPLEMENTAL GUIDANCE**: RP's should request the minimum set of attributes they need in order to function effectively. A privacy risk assessment will help an RP determine the appropriate attributes and the privacy risk associated with those attributes. The privacy risk assessment provides the functional purpose for the requested attributes, identifies the privacy risks arising from the requested attributes, and provides the rationale for any tradeoffs between functionality and privacy risk. **ASSESSMENT OBJECTIVE:** Determine whether RPs have performed a privacy risk assessment when determining which attributes are requested from the IdP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The RP's privacy risk assessment, attribute analyses or assessments, and documented policies for requesting attributes.

ATTR-6	**REQUIREMENT**: The RP SHALL, where feasible, request attribute references rather than full attribute values as described in Section 9.3. (7.3)

	SUPPLEMENTAL GUIDANCE: In some instances, the information the RP needs to operate can be derived from the attributes associated with a subscriber, and the IdP can perform that derivation without releasing the attribute value to the RP. For example, determining whether a subscriber resides in a particular district can be determined by the IdP using the subscriber's physical address without releasing the physical address itself to the RP. This practice minimizes the RP's unnecessary collection of potentially-sensitive information. To fulfill this requirement, the RP needs to determine which attributes are better requested as attribute references and request the IdP for those references when the options are available. The exact attribute references available will vary based on the federation protocol in use, the needs of the RP, and the capabilities of the IdP. The IdP's requirements for this feature are discussed in [ATTR-7]. **ASSESSMENT OBJECTIVE:** Determine whether the RP requests attribute references where feasible. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: RP policy documentation of attribute uses, the configuration and code of the RP to request attribute references instead of full attributes where possible. **Test**: Log in to the RP and examine the use of attribute references in returned information.

ATTR-7	**REQUIREMENT**: The IdP SHALL support attribute references. (7.3) **SUPPLEMENTAL GUIDANCE**: In some instances, the information the RP needs to operate can be derived from the attributes associated with a subscriber, and the IdP can perform that derivation without releasing the attribute value to the RP. For example, determining whether a subscriber resides in a particular district can be determined by the IdP using the subscriber's physical address without releasing the physical address itself to the RP. This practice minimizes the RP's unnecessary collection of potentially-sensitive information. To fulfill this requirement, the RP needs to determine which attributes are better requested as attribute references and request the IdP for those references when the options are available. The exact attribute references available will vary based on the federation protocol in use, the needs of the RP, and the capabilities of the IdP. To fulfill this requirement the IdP needs to determine which attributes are best supported as references for its RPs and make those attribute references available as options. The RP's requirements for this feature are discussed in [ATTR-6]. **ASSESSMENT OBJECTIVE:** Determine whether the IdP supports attribute references. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The configuration, code, and documentation of the IdP to identify all attribute references made available to RPs.

	Test: Log in to an RP using the IdP and examine the use of attribute references in returned information.

3 Identifier Conformance Criteria

All IdPs SHALL be assessed on the following criteria:

ID-1	**REQUIREMENT**: 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. (6) **SUPPLEMENTAL GUIDANCE**: Even if an IdP uses a collision-resistant namespace such as a UUID for its subscriber identifiers, the tying of a specific identifier to a particular subscriber is still under the control of the IdP making the assertion. An RP's internal processing of an assertion needs to take this into account by processing the combination of the subject identifier along with the IdP that issued the assertion. If the RP does not account for the source IdP when determining the identity of the subscriber, a rogue or compromised IdP could impersonate subscribers from another IdP at a susceptible RP by mimicking the valid IdP's subject identifiers. **ASSESSMENT OBJECTIVE:** Determine whether an RP treats the same subject identifier for different IdPs as different accounts. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine:** The RP's code, configuration, and documentation regarding how it handles subject identifiers and ensure that all subject identifiers are taken in the context of the IdP that is asserting the identifier, regardless of the format or contents of the subject identifier. **Test**: Log into an RP from two different IdPs but have both IdPs assert the same subject identifier. Observe that the RP treats both logins as different users and does not associate them together.

ID-2	*If pairwise identifiers are used:* **REQUIREMENT**: When using pairwise pseudonymous subject identifiers within the assertions generated by the IdP for the RP, the IdP SHALL generate a different identifier for each RP as described in Section 6.3.2. (6.3.1) **SUPPLEMENTAL GUIDANCE**: Pairwise identifiers make it more difficult to track a single subscriber across different RPs. The utility of these identifiers relies on a single identifier not being reused at multiple RPs, as doing so would allow two colluding RPs to correlate a single subscriber's actions, negating the usefulness of the pairwise identifier. If pairwise identifiers are not used, this requirement does not apply. The requirements for generation of pairwise identifiers are discussed in [ID-3] and [ID-4]. Specific exceptions to some of the requirements of pairwise identifiers are discussed in [ID-5], [ID-6], and [ID-7]. The use of pairwise identifiers by federation proxies is discussed in [PROXY-3].

	ASSESSMENT OBJECTIVE: Determine whether pairwise identifiers are unique per subscriber-RP combination. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The documentation and generation algorithm used by the IdP to assign a pairwise identifier to a subscriber at an RP. **Test**: Log the same subscriber into two different RPs using the same IdP and ensure that the subject identifier is distinct between them.

ID-3	*If pairwise identifiers are used:* **REQUIREMENT**: Pairwise pseudonymous identifiers SHALL contain no identifying information about the subscriber. (6.3.2) **SUPPLEMENTAL GUIDANCE**: Pairwise identifiers are intended to protect the privacy of the subscriber and prevent collation of subscriber information. If the identifier itself has any identifying information in it, such as a username or employee number, this protection is lost. To prevent this, pairwise identifiers should be random and unguessable values or generated using information known only to the IdP, such as a secret key. If pairwise identifiers are not used, this requirement does not apply. See also [ID-4]. **ASSESSMENT OBJECTIVE:** Determine whether pairwise identifiers contain any identifying information or are predictably generated from identifying information for the subscriber or the RP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The documentation and generation algorithm used by the IdP to assign a pairwise identifier to a subscriber at an RP. **Test**: Log into an RP using a pairwise identifier and examine the generated pairwise identifier against this requirement.

ID-4	*If pairwise identifiers are used:* **REQUIREMENT**: Pairwise pseudonymous identifiers SHALL also be unguessable by a party having access to some information identifying the subscriber. (6.3.2) **SUPPLEMENTAL GUIDANCE**: Pairwise identifiers are intended to protect the privacy of the subscriber and prevent collation of subscriber information. If the identifier itself is easily generated by information known to a party, such as a hash of the username and the RP's identifier, this protection is lost. To prevent this, pairwise identifiers should be random and unguessable values or generated using information known only to the IdP, such as a secret key. If pairwise identifiers are not used, this requirement does not apply. See also [ID-3].

	ASSESSMENT OBJECTIVE: Determine whether pairwise identifiers can be guessed or easily generated by a party with access to subscriber information. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The documentation and generation algorithm used by the IdP to assign a pairwise identifier to a subscriber at an RP. **Test**: Log into an RP using a pairwise identifier and examine the generated pairwise identifier against this requirement.

ID-5	*If pairwise identifiers are used and common pairwise identifiers are requested by RPs:* **REQUIREMENT**: *[Pairwise]* identifiers SHALL only be known by and used by one pair of endpoints (e.g., IdP-RP) *[except under specific circumstances]*. (6.3.2) **SUPPLEMENTAL GUIDANCE**: Pairwise identifiers are intended to separate the information that different RPs know about a given subscriber as discussed in [ID-2]. As such, each pairwise identifier is supposed to be limited to use at a single RP from a single IdP. However, some use cases call for the same pairwise identifier being used for multiple, related RPs. This is distinct from a public identifier, which is used across all RPs, since the common pairwise identifier is only the same for a limited set of specific RPs. An IdP is permitted to produce a common pairwise identifier for multiple different RPs under the following limited circumstances: • 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. The IdP should be able to justify any response it takes to identified privacy risks, including accepting the risk, mitigating the risk, and sharing the risk. In determining when a set of RPs should share a common pairwise pseudonymous identifier as in Section 6.3.2, the IdP considers the subscriber's understanding of such a grouping of RPs and the role of notice in assisting such understanding. If common pairwise identifiers are not used, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine the operational requirement for common pairwise identifiers and establish the consent of the specific RPs in question. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**:

	Examine: The documentation of the operational need for correlations and documentation of consent to be correlated in such a manner from all RPs sharing a common pairwise identifier. The documentation and generation algorithm used by the IdP to assign a common pairwise identifier to a subscriber for a group of related RPs and determine that this algorithm does not generate the same identifier for any RP outside of the group. **Test**: Log the same subscriber into two different RPs that are not configured to use a common identifier at the IdP and ensure that the subject identifier is distinct between them. Log the same subscriber into two different RPs that are configured to use a common identifier at the IdP and ensure that the same subject identifier is used at both.

ID-6	*If pairwise identifiers are used and common pairwise identifiers are requested by RPs:* **REQUIREMENT**: The RPs SHALL conduct a privacy risk assessment to consider the privacy risks associated with requesting a common *[pairwise]* identifier. (6.3.2) **SUPPLEMENTAL GUIDANCE**: If an RP requests a common pairwise identifier as discussed in [ID-5], a privacy risk assessment can help the RP consider the likelihood that requesting the same identifier for a subscriber at multiple RPs could create a problem for the applicant and the impact if a problem did occur. The RP should be able to justify any response it takes to identified privacy risks, including accepting the risk, mitigating the risk, and sharing the risk. If common pairwise identifiers are not used, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether the RPs have conducted a privacy risk assessment before requesting a common identifier. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The RP's policies and practices for requesting a common pairwise identifier.

ID-7	*If pairwise identifiers are used and common pairwise identifiers are requested by RPs:* **REQUIREMENT**: 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. (6.3.2) **SUPPLEMENTAL GUIDANCE**: Since the IdP determines the method for generating the pairwise identifier used at each RP, it is up to the IdP to decide when to give multiple RPs the same pairwise identifier. It is the IdP's responsibility to ensure that only RPs that have been explicitly grouped together

	are given the same identifier. If a pairwise identifier is not used, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether only RPs that have been explicitly configured to use a common identifier are given the common identifier. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The documentation and generation algorithm used by the IdP to assign a pairwise identifier to a subscriber at an RP. **Test**: Log the same subscriber into two different RPs that are not configured to use a common identifier at the IdP and ensure that the subject identifier is distinct between them. Log the same subscriber into two different RPs that are configured to use a common identifier at the IdP and ensure that the same subject identifier is used at both.

4 Identity Provider Conformance Criteria

All Identity Providers SHALL be assessed on the following criteria:

IDP-1	**REQUIREMENT**: Government-operated IdPs asserting authentication at AAL2 and all IdPs asserting authentication at AAL3 SHALL protect keys used for signing or encrypting those assertions with mechanisms validated at FIPS 140 Level 1 or higher. (4.1) **SUPPLEMENTAL GUIDANCE**: This requirement aligns the key storage requirements for the IdP with the key storage requirements needed by the authentication process itself. The requirement for key protection mechanisms validated at FIPS 140 Level 1 or higher for authentication asserted at AAL2 applies only to government-operated IDPs or IDPs operating on behalf of the Federal Government. **ASSESSMENT OBJECTIVE:** Determine whether cryptographic modules used for storage of keying material at the IdP are has been validated at FIPS 140 Level 1 or higher. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The storage mechanisms of keying material at the IdP and ensure that keys cannot be exfiltrated or used by an unauthorized party.

IDP-2	**REQUIREMENT**: 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 subscriber. (4.2) **SUPPLEMENTAL GUIDANCE**: The IdP is a trusted holder of information for the subscriber. When the subscriber is interacting with the IdP, the IdP might need to display some sensitive information to the subscriber to allow the subscriber to confirm and authorize the release of that information to the RP. When doing so, the IdP needs to present that information in such a way as the full value of the sensitive information is not displayed on the screen at default. **ASSESSMENT OBJECTIVE:** Determine whether sensitive information is masked upon display by default. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Navigate the interface of the IdP as a subscriber and observe that sensitive information is masked upon first display. This test needs to include both subscriber-facing administrative pages as well as authorization and consent pages.

IDP-3	**REQUIREMENT**: The IdP SHALL provide mechanisms for the subscriber to temporarily unmask such information in order for the subscriber to view full values. (4.2) **SUPPLEMENTAL GUIDANCE**: When the IdP masks sensitive information as in [IDP-2], the IdP needs to allow the subscriber to temporarily unmask the sensitive information and view the full unmasked value. **ASSESSMENT OBJECTIVE:** Determine whether masked information can be temporarily unmasked. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: View sensitive information at the IdP that has been masked by default and unmask the information.

IDP-4	**REQUIREMENT**: The IdP SHALL provide effective mechanisms for redress of applicant complaints or problems (e.g., subscriber identifies an inaccurate attribute value). (4.2) **SUPPLEMENTAL GUIDANCE**: IdPs need to provide effective mechanisms for redress of applicant complaints or problems arising from the federation (e.g., subscriber identifies an inaccurate attribute value). The Privacy Act requires federal agencies that maintain a system of records to follow procedures to enable applicants to access and, if incorrect, amend their records. Any Privacy Act Statement should include a reference to the applicable SORN(s), which provide the applicant with instructions on how to make a request for access or correction. Non-federal entities should have comparable procedures, including contact information for any third parties if they are the source of the information. **ASSESSMENT OBJECTIVE:** Determine whether the IdP provides effective mechanisms for redress of applicant complaints or problems. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Redress mechanisms for resolving complaints or problems arising from the federation, IdP documentation identifying the means and methods of contacting the IdP for applicant complaints and problems, sample complaint/inquiries to the IdP and documentation of the resolution (e.g., logs). **Test**: Contact the IdP through the published means.

IDP-5	**REQUIREMENT**: 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. (5.1.2) **SUPPLEMENTAL GUIDANCE**: A static registration can be facilitated by system administrators communicating and entering configuration information by

	hand into the software. Since dynamic registration allows for the programmatic introduction of an RP to an IdP, relying on hand configuration is not scalable. To facilitate this, the IdP has to publish its connection and configuration information for the RP software to configure itself and request registration at the IdP. **ASSESSMENT OBJECTIVE:** Determine whether IdP's configuration information is available in a machine-readable and discoverable format. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The IdP's documentation to determine the location of discovery information for the IdP. **Test**: Download the discovery information and use it to configure RP software with the parameters needed to connect to the IdP, including allowing the RP to register itself.

IDP-6	**REQUIREMENT**: If an IdP uses consent measures, then the IdP SHALL NOT make consent for the additional processing a condition of the identity service. (5.2) **SUPPLEMENTAL GUIDANCE**: An IdP's fundamental role is providing identity services on behalf of the subscriber, but an IdP could offer a number of other services to subscribers as part of an overall system. However, the IdP cannot require subscribers to use non-identity services as a bundled part of using the identity service. For example, if an IdP also offers email hosting functionality tied to the subscriber's account, the IdP cannot require the subscriber to use that email service as part of using the federated login functionality. Subscriber consent needs to be meaningful; therefore, when IdPs do use consent measures, they cannot make acceptance by the subscriber of additional services a condition of providing the identity service. Processing of identity information for non-federation purposes that are related to identity (such as security signaling) are discussed in [TRUST-5]. **ASSESSMENT OBJECTIVE**: Determine whether identity services are a separable service and function from other functions provided by the IdP and that a subscriber can decline non-identity services and still use identity services from an IdP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The IdP's documented service policies including functional requirements for all accounts to ensure identity functions can be used without any additional services being required, documentation of UI/UX (e.g., screen shots) showing notice given to subscribers regarding their ability to decline to the processing of their data for non-identity purposes.

	Test: Examine subscriber accounts to ensure an account can be created and used with only identity services.

5 Trust Relationship Conformance Criteria

All IdPs and RPs in a trust agreement or trust framework SHALL be assessed on the following criteria:

TRUST-1	**REQUIREMENT**: The fact that parties have federated SHALL NOT be interpreted as permission to pass information. (4.2) **SUPPLEMENTAL GUIDANCE**: Release of information within a federated login between an IdP and an RP requires two agreements: the agreement to connect in a federation in the first place, and subsequently the agreement to release specific information within that connection. Information release can be subject to allowlists configured at the IdP as well as subscriber-driven runtime decisions, both of which augment the federation configuration itself. **ASSESSMENT OBJECTIVE:** Determine whether every federated login between an IdP and an RP correlates either to an explicit allowlist or to a runtime decision controlling information release. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: If information is released allowing a login, ensure that the RP and the set of released information exists on an allowlist configured at the IdP or that there was a runtime prompt made for the request. **Test**: If possible, connect an RP that is not allowlisted to an IdP and observe either a consent prompt at runtime or the denial of the login request.

TRUST-2	**REQUIREMENT**: A subscriber's information SHALL be transmitted between IdP and RP only for identity federation transactions or support functions such as identification of compromised accounts as discussed in Section 5.2. (4.2) **SUPPLEMENTAL GUIDANCE**: IdPs are trusted holders of identity information and are not allowed to transmit that information to RPs outside of very limited circumstances. In addition to the primary function of federated identity transactions, IdPs and RPs are allowed to transmit a subscriber's information in support of security functions such as identifying an account suspected of compromise or suspicious behavior, as discussed in [TRUST-5]. However, any other transmission of subscriber information is not allowed. **ASSESSMENT OBJECTIVE:** Determine whether the transmission of subscriber information between the IdP and RP is within permissible purposes. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Documented policies and agreements between the IdP and RP regarding subscriber's information processing including permissible purposes,

	sample subscriber transaction data between the IdP and RP, IdP mechanisms to monitor permissible uses of subscriber data.

TRUST-3	*If allowlists are in use:* **REQUIREMENT**: A subscriber's information SHALL NOT be transmitted for any purpose other than identity federation transactions or support functions such as identification of compromised accounts, even when those parties are *[allowlisted]*. (4.2) **SUPPLEMENTAL GUIDANCE**: This requirement is corollary to [TRUST-1] and [TRUST-2] to clarify that allowlisting does not exempt the IdP and RP from these requirements, and they are not allowed to send the subscriber's information outside of approved limited circumstances. **ASSESSMENT OBJECTIVE:** Determine whether the subscriber information is not transmitted outside of allowed purposes. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The configuration and function of the IdP and RP to observe any uses of subscriber information that do not qualify as identity federation or a support function.

TRUST-4	*If the federation relationship between parties is manual or static:* **REQUIREMENT**: Federation relationships SHALL establish parameters regarding expected and acceptable IALs and AALs in connection with the federated relationship. (5.1.1) **SUPPLEMENTAL GUIDANCE**: When an IdP sends an assertion claiming a particular IAL and AAL was used for the subscriber, the RP needs to know that the IdP is actually capable of reaching those levels and is trusted to assert them. The trust agreement between the IdP and RP establishes the minimum and maximum IAL and AAL values for each connection. **ASSESSMENT OBJECTIVE:** Determine whether the federation relationship of the IdP and RP documents the IAL and AAL parameters, establishing upper and lower bounds of each. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The documentation of the federation relationship between the IdP and RP and make sure it contains appropriate IAL and AAL parameters.

TRUST-5	**REQUIREMENT**: If an IdP discloses information on subscriber activities at an RP to any party, or processes the subscriber's information 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. (5.2) **SUPPLEMENTAL GUIDANCE**: By the nature of a federated protocol, the IdP will know which RPs a subscriber logs in to and will know which attributes have been released to which RPs. This information is used as part of the federated login process, identified here as "identity service", to facilitate login to an RP. IdPs need to use measures to maintain the objectives of predictability (enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system) and manageability (providing the capability for granular administration of PII, including alteration, deletion, and selective disclosure) commensurate with privacy risks that can arise from the processing of information for purposes other than identity proofing, authentication, authorization, or attribute assertion, related fraud mitigation, or to comply with law or legal process as in [NISTIR8062]. However, processing information for purposes other than the identity service can create privacy risks when individuals are not expecting or are not comfortable with the additional processing. These exception cases, which are not part of the federated identity protocol process, need to be managed in accordance with the risks associated with such additional processing of the subscriber's information. IdPs can use privacy risk assessments to determine the extent of privacy risks arising from such processing and implement measures commensurate with the privacy risk arising from the additional processing. Such measures may include providing clear notice, obtaining subscriber consent, or enabling selective use or disclosure of attributes, but other measures may be more effective in mitigating the privacy risks depending on the type of processing. **ASSESSMENT OBJECTIVE:** Determine the appropriateness of measures implemented to mitigate privacy risks arising from IdP's additional information processing. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The IdP's policies for information processing, the IdPs privacy risk assessments, and the measures implemented to mitigate identified privacy risks.

TRUST-6	**REQUIREMENT**: 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 Section 9.4). (5.2) **SUPPLEMENTAL GUIDANCE**: This requirement applies to federal agencies. Section 5.2 identifies agency requirements to consult their SAOP to determine privacy compliance requirements. It is critical to involve an agency's SAOP in the earliest stages of digital authentication system development to assess and mitigate privacy risks and advise the agency on compliance obligations such as whether the federation triggers the Privacy Act of 1974 or the E-Government Act of 2002 requirement to conduct a PIA. For example, if the Agency is serving

	as an IdP in a federation, it is likely that the Privacy Act requirements will be triggered and require coverage by either a new or existing Privacy Act system of records since credentials would be maintained at the IdP on behalf of any RP it federates with. If, however, the agency is an RP and using a third-party IdP, digital authentication may not trigger the requirements of the Privacy Act, depending on what data passed from the RP is maintained by the agency as the RP (in such instances the agency may have a broader programmatic SORN that covers such data). Due to the many components of digital authentication, it is important for the SAOP to have an awareness and understanding of each individual component. For example, other privacy artifacts may be applicable to an agency offering or using federated IdP or RP services, such as Data Use Agreements, Computer Matching Agreements, etc. The SAOP can assist the agency in determining what additional requirements apply. Moreover, a thorough understanding of the individual components of digital authentication will enable the SAOP to thoroughly assess and mitigate privacy risks either through compliance processes or by other means. **ASSESSMENT OBJECTIVE:** Determine whether the agency has consulted with its SAOP to determine if the service triggers the requirements of the Privacy Act of 1974, and if applicable see [TRUST-7]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Documentation of consultation with the SAOP regarding applicability of the Privacy Act of 1974, privacy threshold analyses.

TRUST-7	*If the Privacy Act is triggered:* **REQUIREMENT**: The agency SHALL publish or identify coverage by a System of Records Notice (SORN) as applicable. (5.2) **SUPPLEMENTAL GUIDANCE**: This requirement applies to federal agencies participating in federation processes as an IDP or RP directly or through a commercial provider [TRUST-6]. If the SAOP has determined that the Privacy Act is triggered, the agency is required to either publish or identify existing coverage by a SORN. **ASSESSMENT OBJECTIVE:** Determine whether the agency has published a SORN. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Applicable system of records notice.

TRUST-8	**REQUIREMENT**: 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. (5.2)

	SUPPLEMENTAL GUIDANCE: This requirement applies to federal agencies. Section 5.2 identifies agency requirements to consult their SAOP to determine privacy compliance requirements. It is critical to involve the agency's SAOP in the earliest stages of digital authentication system development to assess and mitigate privacy risks and advise the agency on compliance obligations such as whether the federation triggers the Privacy Act of 1974 or the E-Government Act of 2002 requirement to conduct a PIA. The SAOP can assist the agency in determining whether a PIA is required. These considerations should not be read as a requirement to develop a Privacy Act SORN or PIA for use of a federated credential alone. In many cases it will make the most sense to draft a PIA and SORN that encompasses the entire digital authentication process or includes the digital authentication process as part of a larger programmatic PIA that discusses the program or benefit the agency is establishing online access. **ASSESSMENT OBJECTIVE:** Confirm that the agency has consulted with its SAOP to determine the applicability of the E-Government Act to the federation services, and if applicable see [TRUST-9]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Documentation of consultation with the SAOP regarding applicability of the E-Government Act of 2002, privacy threshold analyses.

TRUST-9	*If the E-Government Act is triggered:* **REQUIREMENT**: The agency SHALL publish or identify coverage by a Privacy Impact Assessment (PIA) as applicable. (5.2) **SUPPLEMENTAL GUIDANCE**: This requirement applies to federal agencies participating in federation processes as an IDP or RP directly or through a commercial provider [TRUST-8]. If the SAOP has determined that the E-Government Act is triggered, the agency is required to either publish or identify coverage by a PIA. **ASSESSMENT OBJECTIVE:** Determine whether agency has published a PIA. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The agency's published PIA, as applicable.

6 Federation Authority Conformance Criteria

All federation authorities SHALL be assessed on the following criteria:

FED-1	*If a federation authority is in use:* **REQUIREMENT**: Federation authorities SHALL establish parameters regarding expected and acceptable IALs, AALs, and FALs in connection with the federated relationships they enable. (5.1.3) **SUPPLEMENTAL GUIDANCE**: A federation authority determines the bounding parameters of the actions within a federation, including what xALs are available to all of the participants under the authority. Individual transactions between participants in the federation can use any of the xALs that are enumerated by the authority. The means of the authority publishing the information is not specified. **ASSESSMENT OBJECTIVE:** Determine whether the federation authority has documented the xAL parameters allowed within the federation. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The federation authority's documentation and ensure that both upper and lower bounds are defined for IAL, AAL, and FAL.

FED-2	*If a federation authority is in use:* **REQUIREMENT**: Federation authorities SHALL individually vet each participant in the federation to determine whether they adhere to their expected security, identity, and privacy standards. (5.1.3) **SUPPLEMENTAL GUIDANCE**: The federation authority determines who is allowed within the federation. It is the responsibility of the federation authority to ensure that any participant added to the federation adheres to all appropriate requirements. **ASSESSMENT OBJECTIVE:** Determine whether the federation authority evaluates or otherwise ensures that all participants in the federation adhere to the federation authority's standards. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The documentation of the federation authority's process for adding an IdP or RP to the federation and ensure the federation authority follows that process when doing so.

FED-3	*If a federation authority is in use:* **REQUIREMENT**: Vetting of IdPs and RPs SHALL establish, as a minimum, that assertions generated by IdPs adhere to the requirements in Section 6. (5.1.3)

	SUPPLEMENTAL GUIDANCE: Before adding an IdP to the federation, the federation authority needs to ensure that assertions generated by the IdP meet all the assertion requirements in the document. **ASSESSMENT OBJECTIVE:** Determine whether the federation authority's process for adding an IdP examines and verifies the IdP's assertions. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The documentation for the federation authority's onboarding process for IdPs.

FED-4	*If a federation authority is in use:* **REQUIREMENT**: Vetting of IdPs and RPs SHALL establish, as a minimum, that RPs adhere to IdP requirements for handling subscriber attribute data, such as retention, aggregation, and disclosure to third parties. (5.1.3) **SUPPLEMENTAL GUIDANCE**: Before adding an RP or IdP to the federation, the federation authority needs to ensure that all subscriber information is handled appropriately by the party in question. **ASSESSMENT OBJECTIVE:** Determine whether the federation authority's process for adding an IdP or RP examines and verifies the party's data handling practices. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The documentation for the federation authority's onboarding process for IdPs and RPs.

FED-5	*If a federation authority is in use:* **REQUIREMENT**: Vetting of IdPs and RPs SHALL establish, as a minimum, that RP and IdP systems use approved profiles of federation protocols. (5.1.3) **SUPPLEMENTAL GUIDANCE**: The federation authority determines which profiles of federation protocols are approved for use within the federation and must ensure that all of the participants in the federation use only these profiles. The federation authority needs to determine that IdPs and RPs follow these profiles before they are added to the federation. **ASSESSMENT OBJECTIVE:** Determine whether the federation authority documents acceptable profiles and that IdPs and RPs follow these profiles. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The federation authority's documentation of acceptable profiles and its enforcement of adherence to those profiles.

7 Back-Channel Conformance Criteria

All IdPs and RPs using back-channel presentation mechanisms SHALL be assessed on the following criteria:

BACK-1	*If the assertion is presented in the back-channel:* **REQUIREMENT**: For assertions that are passed directly between IdP and RP, the actual assertion MAY be encrypted. If it is not, the assertion SHALL be sent over an authenticated protected channel. (6.2.3) **SUPPLEMENTAL GUIDANCE**: When an assertion is sent directly from the IdP to the RP, such as by using a back-channel presentation mechanism, the assertion does not need to be encrypted to protect its contents since it is not handled by any additional parties. However, it is still possible to encrypt the assertion itself even in this mode. When the encryption is not directly encrypted, it has to be transmitted over an encrypted channel that ensures its integrity and protects its contents. **ASSESSMENT OBJECTIVE:** Determine whether assertions passed over a back channel between an IdP and RP are protected either by encryption of the assertion itself or by being passed over an authenticated protected channel. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Log in to an RP using a back-channel presentation mechanism and observe the transmission of the assertion from the IdP to ensure that the transmission happens over an authenticated protected channel or that the assertion is encrypted. Attempt to log in to an RP using a back-channel presentation mechanism with an assertion that is not encrypted and has not been passed over an authenticated protected channel and ensure the RP rejects the assertion. The RP can alternatively refuse to connect to the IdP at all unless over an authenticated protected channel.

BACK-2	*If an assertion reference is used:* **REQUIREMENT**: The assertion reference itself contains no information about the subscriber and SHALL be resistant to tampering and fabrication by an attacker. (7.1) **SUPPLEMENTAL GUIDANCE**: Assertion references are used to limit the information that is exposed to different parties within the federation transaction, such as the user's browser. As a consequence, it is counterproductive to put any information about the subscriber in the assertion reference itself. Additionally, since the RP will trade the assertion reference for the actual assertion, the assertion reference needs to be something that an attacker can neither guess nor manipulate in order to alter the assertion received. It is recommended that assertion references be cryptographically random values. If assertion references are not used, this requirement does not apply.

	ASSESSMENT OBJECTIVE: Determine whether the assertion reference contains no information about the subscriber and that it cannot be manipulated or created by an attacker. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The IdP's code and policy for generating assertion references, and for validating assertion references received from an RP. **Test**: Log in to an RP using an assertion reference and ensure the assertion reference contains no information within it about the subscriber.

BACK-3	*If an assertion reference is used:* **REQUIREMENT**: The assertion reference SHALL be limited to use by a single RP. (7.1) **SUPPLEMENTAL GUIDANCE**: Since assertion references are traded for assertions, the IdP needs to ensure that the assertion reference is presented only by the specific RP to which it was issued. Otherwise, an attacker could capture an assertion reference and inject it into a different RP to fake a log in. This requirement applies even if the RPs are logistically related, such as being configured to receive a common identifier. If assertion references are not used, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether assertion references can only be used by a single RP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Start valid log in processes from two different RPs at the same IdP, using assertion references. Intercept the log in process at the RP and inject the assertion reference from the first RP into the second RP's log in process. Ensure that the IdP rejects the invalid assertion reference presented by the second RP and does not issue an assertion.

BACK-4	*If an assertion reference is used:* **REQUIREMENT**: The assertion reference SHALL be single use. (7.1) **SUPPLEMENTAL GUIDANCE**: After an assertion reference is traded for a valid assertion by the RP, a legitimate RP does not have any need to use the assertion reference again. As a consequence, once the trade has occurred there is no need for the IdP to honor that assertion reference again since a legitimate RP would not present it more than once. If assertion references are not used, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether assertion references can be successfully used only once.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Test**: Log in from an RP using an assertion reference. After the RP has submitted the assertion reference successfully and retrieved an assertion, have the RP submit the same assertion reference a second time. Ensure that the IdP does not generate an assertion for the second submission.

BACK-5	*If an assertion reference is used:* **REQUIREMENT**: The RP SHALL protect itself against injection of manufactured or captured assertion references by use of cross-site scripting protection or other accepted techniques. (7.1) **SUPPLEMENTAL GUIDANCE**: The assertion reference needs to be delivered to the RP in some fashion, and for many protocols this happens through a front-channel redirect through the subscriber's browser. The RP needs to ensure that any assertion references presented to it are legitimate by protecting itself against common injection attacks. The techniques for protection vary depending on the type of RP application and its deployment model, but there are many resources and documented best practices for different applications and platforms. For example, ensuring that the assertion reference is returned in the same browser session that was used to request the assertion reference in the front channel. Without these protections, an attacker could convince an RP to trade an injected (but otherwise valid) assertion reference and therefore get a fraudulent assertion and give the attacker access to the RP. If assertion references are not used, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether the RP employs best practices for its platform to protect against injection of assertion references. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Capture an assertion reference for an RP and inject it into an unrelated active session at the RP. Ensure that the RP does not accept the injected assertion reference or attempt to exchange the reference for an assertion.

BACK-6	*If an assertion reference is used:* **REQUIREMENT**: 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. (7.1) **SUPPLEMENTAL GUIDANCE**: In this model, the assertion reference is passed through the front channel using the subscriber's browser. This process consists of two separate network connections over which information flows, from the subscriber to the IdP and the subscriber to the RP. Both legs of this connection have to be protected from attackers by using authenticated protected channels, such as HTTPS over TLS connections.

	ASSESSMENT OBJECTIVE: Determine whether the delivery of the assertion reference occurs over authenticated protected channels, across all connections. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: During delivery of the assertion reference, ensure that both the connection from the browser to the IdP and the connection from the browser to the RP are over authenticated protected channels. Attempt to request and deliver the assertion reference over non-protected channels (such as plain HTTP) and ensure that the request is rejected. Note that the IdP and RP may simply refuse connection entirely over non-protected channels instead of delivering a protocol-specific error.

BACK-7	*If an assertion reference is used:* **REQUIREMENT**: 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. (7.1) **SUPPLEMENTAL GUIDANCE**: In this model, the assertion reference is traded for the assertion by the RP making a direct call to the IdP. This call, which carries both the assertion reference and the assertion itself, needs to be protected from attackers by using an authenticated protected channel, such as HTTPS over TLS connections. **ASSESSMENT OBJECTIVE:** Determine whether the connection between the RP and IdP takes place over an authenticated protected channel. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: During the trading of an assertion reference for an assertion, ensure that the RP connects to the IdP using an authenticated protected channel. Attempt to trade the assertion reference for an assertion over a non-protected channel (such as plain HTTP) and ensure that the request is rejected. Note that the IdP and RP may simply refuse connection entirely over non-protected channels instead of delivering a protocol-specific error.

BACK-8	*If an assertion reference is used:* **REQUIREMENT**: When assertion references are presented, the IdP SHALL verify that the party presenting the assertion reference is the same party that requested the authentication. (7.1) **SUPPLEMENTAL GUIDANCE**: Before issuing an assertion to the RP in exchange for the assertion reference, the IdP needs to ensure that the RP making the exchange request is the same RP that the assertion reference was intended for. Otherwise, an attacker could substitute an assertion reference for one RP in order to get an assertion for a different RP, or trick the subscriber into authorizing one RP only the authorize the attacker's RP. The IdP can do this by associating a specific RP with the assertion reference when the reference is

	created. See also [BACK-3]. If assertion references are not used, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether an assertion reference is bound to a single RP identified by the IdP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Start valid log in processes from two different RPs at the same IdP, using assertion references. Intercept the log in process at the RP and inject the assertion reference from the first RP into the second RP's log in process. Ensure that the IdP rejects the invalid assertion reference presented by the second RP and does not issue an assertion.

8 Front-Channel Conformance Criteria

All IdPs and RPs using front-channel presentation mechanisms SHALL be assessed on the following criteria:

FRONT-1	*If the assertion is presented over the front channel:* **REQUIREMENT**: If the RP is using a front-channel presentation mechanism, as defined in Section 7.2 (e.g., the OpenID Connect Implicit Client profile or the SAML Web SSO profile), it SHALL require FAL2 or greater in order to protect the information in the assertion from disclosure to the browser or other parties in the transaction other than the intended RP. (4) **SUPPLEMENTAL GUIDANCE**: Front channel presentations pass the assertion from the IdP to the RP indirectly through a third-party component. Generally speaking, this component is the subscriber's browser. The browser is not the intended recipient of the assertion, but an unencrypted assertion could nonetheless be read by any party that holds it. This requirement is to prevent information in the assertion leaking to the browser or any equivalent third-party carrier component. If not using a front channel presentation method, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether all assertions passed through front channel are encrypted. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Assertions passed through front channel presentation mechanisms to ensure that the assertion is encrypted to the RP's key.

FRONT-2	*If the assertion is presented over the front channel:* **REQUIREMENT**: The RP SHALL protect itself against injection of manufactured or captured assertions by use of cross-site scripting protection or other accepted techniques. (7.2) **SUPPLEMENTAL GUIDANCE**: The assertion needs to be delivered to the RP in some fashion, and for many protocols this happens through a front-channel redirect through the subscriber's browser. The RP needs to ensure that any assertions presented to it are legitimate by protecting itself against common injection attacks. The techniques for protection vary depending on the type of RP application and its deployment model, but there are many resources and documented best practices for different applications and platforms. Without these protections, an attacker could convince an RP to accept an injected (but otherwise valid) assertion and gain access to the subscriber's account at an RP. **ASSESSMENT OBJECTIVE:** Determine whether the RP employs best practices for its platform to protect against injection of assertions.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Test**: Capture an assertion for an RP and inject it into an unrelated active session at the RP. Ensure that the RP does not accept the injected assertion.

FRONT-3	*If the assertion is presented over the front channel:* **REQUIREMENT**: Communications between the IdP and the RP SHALL be protected in transit using an authenticated protected channel. (7.3) **SUPPLEMENTAL GUIDANCE**: The IdP and RP communicate security-sensitive values such as assertions, assertion references, credentials, and identity information, and these values need to be protected from attackers while in transit by ensuring all communication between the IdP and RP happens over an authenticated protected channel, such as HTTPS over a TLS connection. **ASSESSMENT OBJECTIVE:** Determine whether the connection between the RP and IdP takes place over an authenticated protected channel. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Log in to an RP using an IdP, ensure that the RP connects to the IdP using an authenticated protected channel. Attempt configure elements of the protocol to run over a non-protected channel (such as plain HTTP) and ensure that the request is rejected. Note that the IdP and RP may simply refuse connection entirely over non-protected channels instead of delivering a protocol-specific error.

FRONT-4	*If the assertion is presented over the front channel:* **REQUIREMENT**: Communications between the subscriber and either the IdP or the RP (usually through a browser) SHALL be made using an authenticated protected channel. (7.3) **SUPPLEMENTAL GUIDANCE**: Front channel communications from the IdP and RP to the subscriber communicate security-sensitive values such as assertions, assertion references, credentials, and identity information, and these values need to be protected from attackers while in transit by ensuring all communication between the IdP and RP happens over an authenticated protected channel, such as HTTPS over a TLS connection. **ASSESSMENT OBJECTIVE:** Determine whether the connections between the subscriber and the RP as well as the subscriber and IdP take place over an authenticated protected channel. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Log in to an RP using an IdP, ensure that the subscriber's browser connects to the RP and the IdP using an authenticated protected channel. Attempt configure elements of the protocol to run over a non-protected channel (such as plain HTTP) and ensure that the request is rejected. Note that the IdP

	and RP may simply refuse connection entirely over non-protected channels instead of delivering a protocol-specific error.

9 Cryptographic Method and Key Material Criteria

All IdPs and RPs using cryptographic methods and key material SHALL be assessed on the following criteria:

CRYPTO-1	**REQUIREMENT**: The IdP SHALL employ appropriately-tailored security controls (to include control enhancements) from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. (4) **SUPPLEMENTAL GUIDANCE**: A compromise of the IdP or its cryptographic material would be detrimental to the federation network. As a consequence, the IdP has to employ stringent security controls, and these controls help protect the network as a whole. NIST SP 800-53 rev.5 and SP 800-53B provide a comprehensive catalog of controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs and risk environments for federal information systems. These controls are the operational, technical, and management safeguards to maintain the integrity, confidentiality, and security of federal information systems and are intended to be used in conjunction with the NIST risk management framework outlined in SP 800-37 and SP 800-63-3 section 5, Digital Identity Risk Management. NIST SP 800-53B presents security control baselines determined by the security categorization of the information system (low, moderate or high) from NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems. The moderate and high baseline controls may be considered the starting point for the selection, enhancement, and tailoring of the security controls presented. Guidance on tailoring the control baselines to best meet the organization's risk environment, systems and operations is presented in SP 800-53B section 2.4 Tailoring Baseline Security Controls. While SP 800-53B and other NIST Special Publications in the SP-800-XXX series apply to federal agencies for the implementation of the Federal information Security Modernization (Management) Act (FISMA), non-federal entities providing services for federal information systems may also need to demonstrate appropriate controls and should similarly use SP 800-53 and associated publications as resources. Non-federal entities may be subject to and conformant with other applicable controls systems and processes for information system security (e.g., FEDRAMP, ISO/IEC 27001). SP800-63A allows the application of equivalent controls from such standards and processes to meet conformance with this criterion. **ASSESSMENT OBJECTIVE:** Determine whether the IdP employs the appropriate security controls, in particular ensure that the keying material cannot be exfiltrated or used by an unauthorized party.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: The security controls on the IdP and evaluate them against the given standards.

CRYPTO-2	*If shared keys are used:* **REQUIREMENT**: If the assertion is protected by a MAC using a shared key, the IdP SHALL use a different shared key for each RP. (4.1) **SUPPLEMENTAL GUIDANCE**: Symmetric cryptography requires signature verifiers to have a copy of the same key used to create the signature, which means that verifiers can also create a signature using the key. This requirement ensures that if symmetric cryptography is used to protect assertions, then each RP has a unique key to prevent an RP from creating an assertion targeted at another RP. **ASSESSMENT OBJECTIVE:** Determine whether any symmetric cryptography uses unique keys and that keys are not re-used for multiple RPs. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The IdP's process for assigning symmetric keying material to an RP to ensure that the assigned keys are unique and not re-used for multiple RPs. **Test**: Present an assertion generated for one RP to another RP and ensure the signature validation fails. Note that other checks for other requirements should also fail in this case.

CRYPTO-3	*If key information needs to be transferred:* **REQUIREMENT**: 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. (5.1.1) **SUPPLEMENTAL GUIDANCE**: [Same as CRYPTO-5] Both the IdP and RP need access to cryptographic keying materials to validate signatures and encrypt content. The association of these keys with specific parties is vital to the security of the protocol. In order to prevent an attacker impersonating an IdP or RP, all keys have to be transferred using secure methods. Methods include the publication of asymmetric public keys over HTTPS (and therefore TLS) at a well-known and trusted URL associated with the IdP or RP, or the use of TLS to transfer keying material in the registration process. Alternatively, keys could be transferred and configured manually by administrators to ensure a strong mapping between the intended party and the value of the key itself. **ASSESSMENT OBJECTIVE:** Determine whether any keying material is transmitted using a secure method.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: The exchange of keying material during a registration process to ensure that all keys and secrets are transmitted securely. **Test**: Register an RP at the IdP and observe how keys are transmitted to the IdP and from the IdP during this process. Ensure that all transmission methods are secured.

CRYPTO-4	*If symmetric keys are used:* **REQUIREMENT**: Any symmetric keys used for federation transactions SHALL be unique to a pair of federation participants. (5.1.1) **SUPPLEMENTAL GUIDANCE**: [Same as CRYPTO-6] Since symmetric keys allow for both the creation and verification of both signed and encrypted content by all parties who possess the key, it's important that any symmetric keys be limited to use between only a single pair of connected parties. If symmetric keys are made available to any other parties, those parties can impersonate each other. **ASSESSMENT OBJECTIVE:** Determine whether the IdP issues different symmetric keys to every party. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Register two RPs and compare the shared keys issued to each to determine they are distinct.

CRYPTO-5	*If key information needs to be transferred:* **REQUIREMENT**: Protocols requiring the transfer of keying information SHALL use a secure method during the registration process to establish such keying information needed to operate the federated relationship, including any shared secrets or public keys. (5.1.2) **SUPPLEMENTAL GUIDANCE**: [same as CRYPTO-3] Both the IdP and RP need access to cryptographic keying materials to validate signatures and encrypt content. The association of these keys with specific parties is vital to the security of the protocol. In order to prevent an attacker impersonating an IdP or RP, all keys have to be transferred using secure methods. Methods include the publication of asymmetric public keys over HTTPS (and therefore TLS) at a well-known and trusted URL associated with the IdP or RP, or the use of TLS to transfer keying material in the registration process. Alternatively, keys could be transferred and configured manually by administrators to ensure a strong mapping between the intended party and the value of the key itself. **ASSESSMENT OBJECTIVE:** Determine whether any keying material is transmitted using a secure method.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: The exchange of keying material during a registration process to ensure that all keys and secrets are transmitted securely. **Test**: Register an RP at the IdP and observe how keys are transmitted to the IdP and from the IdP during this process. Ensure that all transmission methods are secured.

CRYPTO-6	*If symmetric keys are used:* **REQUIREMENT**: Any symmetric keys used for federation transactions SHALL be unique to a pair of federation participants. (5.1.2) **SUPPLEMENTAL GUIDANCE**: [Same as CRYPTO-4] Since symmetric keys allow for both the creation and verification of both signed and encrypted content by all parties who possess the key, it's important that any symmetric keys be limited to use between only a single pair of connected parties. If symmetric keys are made available to any other parties, those parties can impersonate each other. **ASSESSMENT OBJECTIVE:** Determine whether the IdP issues different symmetric keys to every party. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Register two RPs and compare the shared keys issued to each to determine they are distinct.

CRYPTO-7	*If symmetric keys are used:* **REQUIREMENT**: 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. (6.2.2) **SUPPLEMENTAL GUIDANCE**: The nature of symmetric cryptography is such that any party with access to the keying material needed to validate the signature can also create a valid signature. By requiring all symmetric keys used for signing purposes to be unique per RP, this requirement prevents an RP from creating an assertion targeted at a different RP but signed with its own key. See also [CRYPTO-4] and [CRYPTO-6]. If shared symmetric keys are not used, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether any shared symmetric keys are unique per RP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The code and configuration of the IdP and any two independent RPs to determine the uniqueness of shared symmetric keys.

	Test: Have one RP generate a fake assertion using its own shared symmetric key and present that assertion to a second RP, and ensure the second RP rejects the signature.

CRYPTO-8	**REQUIREMENT**: Approved cryptography SHALL be used. (6.2.2) **SUPPLEMENTAL GUIDANCE**: Only approved cryptographic algorithms, key sizes, and methods can be used to sign assertions. **ASSESSMENT OBJECTIVE:** Determine whether approved cryptography is used and unapproved cryptography is rejected. SP 800-63-3 Appendix A defines approved cryptography as: Federal Information Processing Standard (FIPS)-approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The code, configuration, and documentation of the IdP and RP to determine that only approved cryptography is used to sign assertions. **Test**: Generate an assertion and ensure the assertion signature from the IdP uses approved cryptography. Generate an assertion for an RP using cryptography that is not approved (such as an unapproved algorithm or a short key length) and ensure that the RP rejects it.

10 Assertion Signature Conformance Criteria

All IdPs signing assertions and RPs validating assertion signatures SHALL be assessed on the following criteria:

SIG-1	**REQUIREMENT**: At any FAL, the IdP SHALL ensure that an RP is unable to impersonate the IdP at another RP by protecting the assertion with a signature and key using approved cryptography. (4.1) **SUPPLEMENTAL GUIDANCE**: All assertions have to be signed by the IdP in such a way as to prevent an attacker, including a compromised RP, from creating a new assertion directed at a different RP. This can be accomplished by using asymmetric cryptography with a private key known only to the IdP or by using symmetric cryptography with a key shared only between the IdP and a single RP. **ASSESSMENT OBJECTIVE:** Determine whether assertions are signed using appropriate cryptography. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Assertions generated by the IdP and determine the cryptography used.

SIG-2	**REQUIREMENT**: Assertions SHALL be cryptographically signed by the issuer (IdP). (6.2.2) **SUPPLEMENTAL GUIDANCE**: The IdP uses a signature to protect the contents of the assertion from modification by an attacker, and to prevent an attacker from creating a fraudulent assertion. Every assertion issued by the IdP needs to be signed and the signature attached to the assertion for transit and processing by the RP. **ASSESSMENT OBJECTIVE:** Determine whether assertions are signed by the IdP using appropriate cryptography. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Have the IdP issue an assertion and examine that the assertion includes a digital signature or MAC.

SIG-3	**REQUIREMENT**: The RP SHALL validate the digital signature or MAC of each such assertion based on the issuer's key. (6.2.2) **SUPPLEMENTAL GUIDANCE**: It is not sufficient for the assertion to have a signature, the signature itself needs to have been made by the correct party (the IdP) and be valid for the signed content of the assertion. The RP is required to validate the signature as part of its processing.

	ASSESSMENT OBJECTIVE: Determine whether the RP validates the signature or MAC of an assertion. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Deliver an assertion with an invalid signature but otherwise correct payload (not expired, valid issuer, valid audience, etc.) to the RP and ensure the RP rejects the assertion.

SIG-4	**REQUIREMENT**: This signature SHALL cover the entire assertion, including its identifier, issuer, audience, subject, and expiration. (6.2.2) **SUPPLEMENTAL GUIDANCE**: Some signature mechanisms allow for selective coverage of the signature, placing some items outside of the cryptographic protection. This requirement specifies that all the required fields and vital information of the assertion need to be covered by the signature mechanism in use. **ASSESSMENT OBJECTIVE:** Determine whether the signature method used to protect the assertion covers all required components. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Have the IdP generate an assertion and ensure that all required assertion components are covered by the signature. Modifying the value of any required component will invalidate the signature, ensure that an RP rejects such a signature. If the signature mechanism allows for selective coverage of data, generate an otherwise valid assertion with one or more required pieces of information (such as the issuer, subject, or expiration timestamp) outside of the signature. Ensure that an RP rejects such assertions.

SIG-5	**REQUIREMENT**: 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. (6.2.2) **SUPPLEMENTAL GUIDANCE**: This standard defines two mechanisms for protecting an assertion with a signature, based on common cryptographic methods and key types. Other cryptographic signature methods are not defined by this standard and their use is not supported. **ASSESSMENT OBJECTIVE:** Determine whether the signature method used to protect the assertion and the keys used to create and verify it falls under one of these defined categories. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The code and configuration of the IdP that controls assertion signature generation.

	Test: Generate an assertion from the IdP and examine its signature method and key source.

11 FAL2 Conformance Criteria

All IdPs and RPs operating at FAL2 (or above) using encrypted assertions SHALL be assessed on the following criteria:

FAL2-1	*If the assertion is encrypted:* **REQUIREMENT**: When encrypting assertions, the IdP SHALL encrypt the contents of the assertion using either the RP's public key or a shared symmetric key. (6.2.3) **SUPPLEMENTAL GUIDANCE**: Assertions at FAL2 and FAL3 are encrypted to protect the contents. This standard defines two mechanisms for protecting an assertion with encryption, based on common cryptographic methods and key types. When using asymmetric encryption, the assertion has to be targeted specifically to the RP's public key by the IdP. Other cryptographic encryption methods are not defined by this standard and their use is not supported. If an assertion is not encrypted, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether the encryption method used to protect the assertion and the keys used to create and verify it falls under one of these defined categories. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The code and configuration of the IdP that controls assertion encryption. **Test**: Generate an assertion from the IdP and examine its encryption method and key source.

FAL2-2	*If the assertion is encrypted and shared symmetric keys are used:* **REQUIREMENT**: 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. (6.2.3) **SUPPLEMENTAL GUIDANCE**: Assertions at FAL2 and FAL3 are encrypted to protect the contents. The nature of symmetric cryptography is such that any party with access to the key material needed to decrypt the content can also encrypt new content with the same key. By requiring all symmetric keys used for encryption purposes to be unique per RP, this requirement prevents an RP from creating an assertion targeted at a different RP but encrypted with its own key. If an assertion is not encrypted, this requirement does not apply. If the encryption method uses asymmetric keys, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether any shared symmetric keys are unique per RP.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: The code and configuration of the IdP and any two independent RPs to determine the uniqueness of shared symmetric keys. **Test**: Have one RP generate a fake assertion using its own shared symmetric key and present that assertion to a second RP, which will be unable to decrypt the assertion.

FAL2-3	*If the assertion is encrypted:* **REQUIREMENT**: All encryption of assertions SHALL use approved cryptography. (6.2.3) **SUPPLEMENTAL GUIDANCE**: Only approved cryptographic algorithms, key sizes, and methods can be used to encrypt assertions. SP 800-63-3 Appendix A defines approved cryptography as: Federal Information Processing Standard (FIPS)-approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation. **ASSESSMENT OBJECTIVE:** Determine whether approved cryptography is used and unapproved cryptography is rejected. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The code, configuration, and documentation of the IdP and RP to determine that only approved cryptography is used to encrypt assertions. **Test**: Generate an assertion and ensure the assertion encryption from the IdP uses approved cryptography. Generate an assertion for an RP using cryptography that is not approved (such as an unapproved algorithm or a short key length) and ensure that the RP rejects it.

FAL2-4	**REQUIREMENT**: When assertions are passed through third parties, such as a browser, the actual assertion SHALL be encrypted. (6.2.3) **SUPPLEMENTAL GUIDANCE**: Assertions contain sensitive information about the subscriber, including information about the authentication event as well as identity information and personal attributes. This information is targeted to the RP, but unless the assertion is encrypted to the RP, anyone with access to the assertion will be able to read the attributes therefore learning information about the subscriber. Even if the assertion cannot be used by an attacker to impersonate the subscriber or attack the RP, the contents of the assertion could be enough for the attacker to harm the subscriber. To prevent this, whenever using a federation presentation method that passes the assertion through a party that is not the IdP or the RP, such as a front channel presentation that uses the subscriber's browser to deliver the assertion, the assertion has to be encrypted to protect its contents from leaking to unintended participants. If the assertion is

	passed directly from the IdP to the RP, such as through a back-channel presentation, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether assertions passed through the front channel are encrypted. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Log in to an RP using a front channel presentation mechanism and examine the assertion used to ensure that it is encrypted. Attempt to log in to an RP using a front channel presentation mechanism and an unencrypted assertion and ensure the RP rejects the assertion on the basis of the assertion lacking encryption.

13 FAL3 Conformance Criteria

All IdPs and RPs operating at FAL3 with holder-of-key assertions SHALL be assessed on the following criteria:

FAL3-1	*If the assertion is holder-of-key:* **REQUIREMENT**: The subscriber SHALL prove possession of that key to the RP, in addition to presentation of the assertion itself. (6.1.2) **SUPPLEMENTAL GUIDANCE**: Holder-of-key assertions are built around proving that a subscriber is not only known to the IdP, and therefore able to get an assertion issued, but also able to present proof of a cryptographic key in the assertion. This key represents the subscriber, not the IdP or the RP, and the proof of possession of the key is presented by the subscriber directly to the RP. This requirement does not assume that the RP has registered the key for the subscriber, and the subscriber key might be unknown to the RP ahead of processing the assertion. Additionally, the technology in place might use different keys for a subscriber over time. Because of these aspects, the RP needs to validate the subscriber's key separately upon login. **ASSESSMENT OBJECTIVE:** Determine whether the RP validates the subscriber's key for holder-of-key assertions. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Log in to an RP with a holder-of-key assertion. Ensure the RP prompts for the key. Presenting the right key should accomplish a login at FAL3. Presenting the wrong key or no key at all should result in an error.

FAL3-2	*If the assertion is holder-of-key:* **REQUIREMENT**: An assertion containing a reference to a key held by the subscriber for which key possession has not been proven SHALL be considered a bearer assertion by the RP. (6.1.2) **SUPPLEMENTAL GUIDANCE**: The RP can start its session management as soon as it processes an assertion, even an assertion that includes a holder-of-key reference. The mere presence of reference to a subscriber's key in an assertion is not sufficient for reaching FAL3, and the RP has to both validate the assertion as well as confirm that the subscriber holds the key referenced in the assertion before establishing FAL3. The RP can choose to delay prompting for and processing the subscriber's key, but doing results in the assertion not being fully validated as holder-of-key and therefore not reaching FAL3. Otherwise, an attacker could steal a holder-of-key assertion and reach FAL3 without presenting the referenced key.

	ASSESSMENT OBJECTIVE: Determine whether the RP treats an assertion containing a key as sufficient for reaching FAL3 without validating that key with the subscriber. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Log in to an RP with a holder-of-key assertion. If the RP prompts for the key, presenting the right key should accomplish a login at FAL3. If the RP does not prompt for the key, the login should be treated as FAL1 or FAL2 by the RP.

FAL3-3	*If the assertion is holder-of-key:* **REQUIREMENT**: Reference to a given key SHALL be trusted at the same level as all other information within the assertion. (6.1.2) **SUPPLEMENTAL GUIDANCE**: Being able to validate a key within an assertion is not sufficient for establishing a federated connection if the assertion itself is not sufficiently validated. All elements in an assertion are protected by a cryptographic envelope, including a signature and encryption at FAL3. Any keys referenced within an assertion for holder-of-key purposes can only be trusted by the RP at the level of the rest of the assertion. Therefore, the RP needs to validate the assertion and ensure that all operations use approved cryptography. Otherwise, an attacker could substitute their key to get a naïve RP to accept an assertion at FAL3. **ASSESSMENT OBJECTIVE:** Determine whether the RP validates the assertion in addition to the key presented within the assertion. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Present an invalid holder-of-key assertion that contains a valid assertion reference to the RP and ensure the RP does not accept it as a valid login. For example, the invalid assertion could have an incorrect signature or be expired.

FAL3-4	*If the assertion is holder-of-key:* **REQUIREMENT**: The assertion SHALL NOT include an unencrypted private or symmetric key to be used with holder-of-key presentation. (6.1.2) **SUPPLEMENTAL GUIDANCE**: The security of holder-of-key assertions stems from the separation of the key representing the subscriber and the assertion itself. The RP will need access to some set of keying material to verify the key presented by the subscriber in a holder-of-key assertion. There are different methods of identifying this keying material to the RP, such as including the public key of an asymmetric key pair in the assertion or including an identifier for a key that the RP can securely dereference. However, if the assertion were to include private key material or a symmetric key, then any reader of the assertion would be able to create a proof to present alongside the assertion. Therefore, these types of keys are not allowed to be included in the assertion in holder-of-key presentations.

	ASSESSMENT OBJECTIVE: Determine whether the subscriber keys present in a holder-of-key assertion are of an appropriate type. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Generate a holder-of-key assertion and ensure that the assertion does not include an unencrypted private key or symmetric key as the subscriber key.

14 Proxy Conformance Criteria

All identity proxies (also known as identity brokers) SHALL be assessed on the following criteria:

PROXY-1	*If a federation proxy is in use:* **REQUIREMENT**: Federations presented through a proxy SHALL be represented by the lowest level used during the proxied transaction. (4) **SUPPLEMENTAL GUIDANCE**: When using a proxy, different federation processes could be used on either side of the proxy. To avoid accidental upgrading of the transaction giving a false perception of security, the overall FAL for the transaction is limited to the lowest FAL used on either side of the proxy. For example, if FAL1 is used inbound to the proxy, but FAL2 (assertion encryption) is used outbound from the proxy, the proxy has to report the entire transaction at FAL1 to the downstream RP. **ASSESSMENT OBJECTIVE:** Determine whether a proxy does not mask a lower level FAL from its inbound side. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Send an assertion to the proxy at its lowest supported level and request the outbound assertion at its highest level and determine that the resulting assertion from the proxy is at the lower level.

PROXY-2	*If a federation proxy is in use:* **REQUIREMENT**: 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. (5.1.4) **SUPPLEMENTAL GUIDANCE**: A proxy needs to fulfill all of the normative requirements for both RPs and IdPs in order to be considered compliant, in addition to any proxy-specific requirements. **ASSESSMENT OBJECTIVE:** Determine whether a proxy functions as both a compliant IdP and a compliant RP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Test both the RP and IdP interfaces of the proxy to ensure the proxy is functioning in both dimensions as appropriate.

PROXY-3	*If a federation proxy is in use and pairwise identifiers are in use:* **REQUIREMENT**: 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. (6.3.1) **SUPPLEMENTAL GUIDANCE**: This requirement applies in instances where the proxy is generating a pairwise identifier for the downstream RP in order to hide the identifier used by the upstream IdP. Since the proxy generates the pairwise identifier in the context of the request, the proxy will have a mapping between these identifiers. In such cases, if the proxy were to disclose the mapping between the original identifier (now hidden) and the generated pairwise identifier, the pairwise identifier would no longer serve its intended purpose to hide the original identifier from the RP. Disclosure of this mapping is allowed only under the specific exceptions listed in the requirement. Requirements for the generation of pairwise identifiers are discussed further in [ID-2] and related requirements. If a proxy is not used, this requirement does not apply. If pairwise identifiers are not used, this requirement does not apply. If the proxy is not the party generating a pairwise identifier, this requirement does not apply. **ASSESSMENT OBJECTIVE**: Determine whether the proxy discloses the mapping of a pairwise identifier **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The proxy's policies for information disclosure and determine the practices for all allowed categories require protection measures.

15 Allowlist Conformance Criteria

All IdPs and RPs using lists of pre-approved parties and circumstances (also known as an "allowlist" or, formerly, a "whitelist") SHALL be assessed on the following criteria:

ALLOW-1	*If an IdP uses an allowlist to manage federation connections:* **REQUIREMENT**: All RPs in an IdP's *[allowlist]* SHALL abide by the provisions and requirements in the SP 800-63 suite. (4.2) **SUPPLEMENTAL GUIDANCE**: Before an IdP adds an RP to its allowlist, the IdP needs to ensure that the RP follows all of the requirements listed in the suite. As a result, only compliant RPs should ever be found on any IdP's allowlist. However, an RP getting added to an IdP's allowlist does not automatically make the RP beholden to the requirements of the suite as a result of the IdP's action. **ASSESSMENT OBJECTIVE:** Determine whether RPs in an IdP's allowlist are compliant with this suite. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The process an IdP uses to add an RP to the allowlist and determine that the process ensures compliance with the suite for the RP being evaluated for addition. **Test**: Several representative entries of the allowlist to ensure they are compliant with the requirements of this suite.

ALLOW-2	*If an IdP uses an allowlist to manage federation connections:* **REQUIREMENT**: IdPs SHALL make *[allowlists]* available to subscribers as described in Section 9.2. (4.2) **SUPPLEMENTAL GUIDANCE**: When an RP is allowlisted by an IdP, some subset of the subscriber's information is made available to the RP during the login process without the subscriber being prompted at runtime for additional consent or confirmation. The IdP needs to make the list of allowlisted RPs available to subscribers to allow subscribers to view which sites their information will be sent to during a federation transaction without the subscriber being specifically prompted. **ASSESSMENT OBJECTIVE:** Determine whether the list of allowlisted RPs is available to subscribers. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Have a subscriber request the allowlist from the IdP and ensure that this is the full list that applies to the subscriber.

ALLOW-3	*If an RP uses an allowlist to manage federation connections:*

	REQUIREMENT: All IdPs in an RP's *[allowlist]* SHALL abide by the provisions and requirements in the 800-63 suite. (4.2) **SUPPLEMENTAL GUIDANCE**: Before an RP adds an IdP to its decision allowlist, the RP needs to ensure that the IdP follows all of the requirements in the suite. The result of this is that all IdPs in an RP's allowlist are conformant with the requirements of the suite. An IdP being placed on an RP's allowlist does not obligate that IdP to follow the requirements of the suite as a result of the RP's action. **ASSESSMENT OBJECTIVE:** Determine whether all IdPs in an RP's allowlist are compliant with the requirements of this suite. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: The process an RP uses to add an IdP to the allowlist and determine that the process ensures compliance with the suite for the IdP being evaluated for addition. **Test**: Several representative entries of the allowlist to ensure they are compliant with the requirements of this suite.

16 Runtime Decision Conformance Criteria

All IdPs and RPs using decisions made at runtime by an authorized party SHALL be assessed on the following criteria:

RUNTM-1	**REQUIREMENT**: Every RP not on an allowlist or a blocklist SHALL be placed by default in a gray area where runtime authorization decisions will be made by an authorized party, usually the subscriber. (4.2) **SUPPLEMENTAL GUIDANCE**: If a given RP is allowed to request a connection from an IdP, and that RP has not been allowlisted by the IdP, then the IdP needs to prompt the subscriber (or their surrogate, such as an administrator) during the transaction to gather consent for the information release. The purpose of this requirement is to allow subscriber-driven connection decisions where possible in addition to traditional pre-negotiated connections enabled by allowlists. **ASSESSMENT OBJECTIVE:** Determine whether a request for information release by an RP that is not allowlisted triggers a prompt at runtime. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Have an RP that is not allowlisted request information for a subscriber and ensure the prompt is shown and is functional (i.e., the subscriber can both approve or deny the request).

RUNTM-2	*If an IdP can remember the result of a subscriber's runtime decisions:* **REQUIREMENT**: The IdP MAY remember a subscriber's decision to authorize a given RP, provided that the IdP SHALL allow the subscriber to revoke such remembered access at a future time. (4.2) **SUPPLEMENTAL GUIDANCE**: When the IdP allows the subscriber to make a decision to connect to a given RP at runtime, the IdP is allowed to remember the subscriber's decision to authorize that RP such that the subscriber is not prompted for consent again by the IdP when visiting that RP again in the future. If an IdP offers such memory functionality, it has to allow the subscriber to revoke that decision such that the subscriber would be prompted for consent upon visiting that RP again in the future. If an IdP does not offer such memory functionality, this requirement does not apply. **ASSESSMENT OBJECTIVE:** Determine whether a previous runtime decision can be revoked by the subscriber. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Approve an RP that is not allowlisted at runtime and have the IdP remember that decision. Create a new login with that same RP again and ensure the subscriber is not prompted, indicating the decision was remembered. Use the

	IdP's revocation functionality to revoke that memory decision. Create a new login with that same RP a third time and ensure the subscriber is prompted, indicating the remembered decision has been cleared.

RUNTM-3	**REQUIREMENT**: Every IdP that is not on an *[allowlist]* or a *[blocklist]* SHALL be placed by default in a gray area where runtime authorization decisions will be made by an authorized party, usually the subscriber. (4.2) **SUPPLEMENTAL GUIDANCE**: For all IdPs that an RP is allowed to connect with, if the IdP is not allowlisted by the RP then the subscriber (or their surrogate, such as an administrator) will be prompted whether to request a federated login from the IdP. This can take the form of allowing the subscriber to type in a directed identifier to facilitate a discovery process, or the subscriber using an account chooser component to select from their own set of IdPs to present to the RP. **ASSESSMENT OBJECTIVE:** Determine whether a request to login to an IDP that is not allowlisted can be triggered by a prompt at runtime. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Have a subscriber indicate an IDP that is not allowlisted to the RP for a login and observe that the RP allows this input.

RUNTM-4	*If an RP can remember a subscriber's runtime decision:* **REQUIREMENT**: The RP MAY remember a subscriber's decision to authorize a given IdP, provided that the RP SHALL allow the subscriber to revoke such remembered access at a future time. (4.2) **SUPPLEMENTAL GUIDANCE**: When the RP allows the subscriber to make a decision to connect to a given IdP at runtime, the RP is allowed to remember the subscriber's decision to authorize that IdP such that the subscriber is not prompted for consent again by the RP when using that IdP again in the future. If an RP offers such memory functionality, it has to allow the subscriber to revoke that decision such that the subscriber would be prompted for consent upon using that IdP again in the future. **ASSESSMENT OBJECTIVE:** Determine whether a previous runtime decision can be revoked by the subscriber. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Have the subscriber indicate an IDP that is not allowlisted for login at an RP and indicate to remember the decision. Have the subscriber log into the RP again and observe that the IdP was chosen without prompting (indicating the decision was remembered). Revoke the decision at the RP. Have the subscriber log into the RP again and observe that the IdP must now be indicated (indicating that the previously-remembered decision was revoked).

RUNTM-5	**REQUIREMENT**: When the subscriber is involved in a runtime decision, the subscriber SHALL receive explicit notice and be able to provide positive confirmation before any attributes about the subscriber are transmitted to any 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 Section 9.2. (4.2) **SUPPLEMENTAL GUIDANCE**: In order to efficiently facilitate runtime decisions by the subscriber, the subscriber needs to be notified and prompted directly during the course of the federated transaction. Most commonly, this comes in the form of an explicit prompt for the release of information by the IdP to the RP. **ASSESSMENT OBJECTIVE:** Determine whether the subscriber is notified about any information release decisions made during a federated transaction and can provide positive confirmation. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: Content of the prompt provided to the subscriber (e.g., screen shots). **Test**: Have the subscriber log in and trigger a runtime decision to release information and observe an explicit consent request that includes a list of attributes being sent and their values. Observe that the subscriber has the choice to at least accept or deny this request.

RUNTM-6	**REQUIREMENT**: In cases where an RP is not allowlisted, the IdP SHALL require runtime decisions (see Section 4.2) to be made by an authorized party (such as the subscriber) before releasing user information. (5.1.1) **SUPPLEMENTAL GUIDANCE**: This is related to [RUNTM-1]. If the IdP has not allowlisted a given RP for release of requested subscriber information, the IdP prompts the subscriber (or their surrogate, such as an administrator) whether to authorize the release of this information to the RP. **ASSESSMENT OBJECTIVE:** Determine whether a request for information release by a RP that is not allowlisted triggers a prompt at runtime. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Have an RP that is not allowlisted request information for a subscriber and ensure the prompt is shown and is functional (i.e., the subscriber can both approve or deny the request).

RUNTM-7	**REQUIREMENT**: IdPs SHALL require runtime decisions (see Section 4.2) to be made by an authorized party (such as the subscriber) before releasing user information. (5.1.2)

	SUPPLEMENTAL GUIDANCE: An IdP-controlled allowlist does not apply to a dynamically registered RP. For dynamically registered RPs, the subscriber (or their surrogate, such as an administrator) has to explicitly approve the request for subscriber information and consent to the login. **ASSESSMENT OBJECTIVE:** Determine whether the subscriber is prompted before information is released. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Have a dynamically-registered RP request information for a subscriber and ensure the prompt is shown and is functional (i.e., the subscriber can both approve or deny the request).

17 Session Management Conformance Criteria

All IdPs and RPs using session management SHALL be assessed on the following criteria:

SESS-1	**REQUIREMENT**: The RP SHALL NOT assume that the subscriber has an active session at the IdP past the establishment of the federated log in. (5.3) **SUPPLEMENTAL GUIDANCE**: Session lifetimes in a federated system are not bound to each other, as the IdP and RP each manage their authentications and sessions separately. Logging in to the RP does not imply a continued logged-in state at the IdP. The federated log in at the RP occurs due to the presentation of an assertion, and the assertion is generated in the context of an authenticated session at the IdP. However, the assertion represents a specific moment in time; as soon as the assertion is created, the session at the IdP could be terminated without any effect on the RP or assertion. Therefore, the RP can only assume that the subscriber was authenticated at the IdP when the assertion was created and cannot assume any state after. **ASSESSMENT OBJECTIVE:** Determine whether policies, documentation, and function of the RP assumes that sessions at the RP is bound to the session at the IdP. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Examine**: RP messaging to subscribers. **Test**: Perform several log in / log out cycles at an RP while in different authentication states at the IdP.

SESS-2	**REQUIREMENT**: 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. (5.3) **SUPPLEMENTAL GUIDANCE**: Session lifetimes in a federated system are not bound to each other, as the IdP and RP each manage their authenticated sessions separately. Logging out of the IdP does not imply being logged out of any RPs. Sessions at RPs are started as the result of processing the assertion, but the RP session will last much longer than the lifetime of the assertion. While some federation protocols do have mechanisms for signaling RPs that a federated session should be terminated, the RP could either miss or ignore such a signal and continue the session for the subscriber. The IdP can help manage expectations with appropriate training and messaging to the subscriber. **ASSESSMENT OBJECTIVE:** Determine whether policies, documentation, and function of the IdP assumes that sessions at the RP is bound to the session at the IdP.

	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: IdP messaging to subscribers upon logout at the IdP and RP behavior post IdP log out. **Test**: Log in to an RP. Log out of the IdP and observe behaviors at RPs.

SESS-3	**REQUIREMENT**: A timestamp indicating when the assertion expires and SHALL no longer be accepted as valid by the RP (i.e., the expiration of the assertion and not the expiration of the session at the RP). (6) **SUPPLEMENTAL GUIDANCE**: Assertions are statements made at a specific point in time that a particular subscriber is present and authenticated. As such, assertions are naturally time-bound artifacts. The expiration timestamp of an assertion allows an IdP to limit the amount of time that it will be accepted by RPs. RPs need to reject assertions that are presented past their expiration time. **ASSESSMENT OBJECTIVE:** Determine whether the RP rejects an expired assertion. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Generate an assertion for an RP that is expired but otherwise valid and ensure that the RP does not create an authenticated session as a result. This could be accomplished by intercepting the assertion before the RP has processed it and releasing it to the RP only after expiration has occurred, setting the clock on the IdP into the past such that it generates assertions that have already expired from the perspective of the RP, or setting the clock of the RP into the future such that valid assertions from the IdP are seen as expired from its perspective.

SESS-4	**REQUIREMENT**: After the RP consumes the assertion, session management by the RP comes into play (see SP 800-63B Section 7); an assertion SHALL NOT be used past the expiration time contained therein. (6) **SUPPLEMENTAL GUIDANCE**: The lifetime of the assertion is not intended to put an upper bound on the session lifetime at the RP, but a session at the RP cannot start without a valid assertion. Assertions are statements made at a specific point in time that a particular subscriber is present and authenticated. RPs need to reject assertions that are presented past their expiration time. **ASSESSMENT OBJECTIVE:** Determine whether the RP rejects expired assertions and if the expired assertion is used to start or extend a session. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Attempt to log in to an RP with an expired assertion and ensure that the RP does not start an authenticated session as a result.

SESS-5	**REQUIREMENT**: Assertion lifetimes SHALL NOT be used to limit the session at the RP. (6) **SUPPLEMENTAL GUIDANCE**: Assertions are intended to be short-lived statements about a subscriber's presence, and therefore are usually valid only for a short amount time after their issuance. The subscriber's session at the RP is likely to continue long after a typical assertion would expire. If an RP were to use an assertions expiration to limit its own internal session management, there would be pressure on IdPs to generate assertions with significantly longer lifetimes than is considered good practice. **ASSESSMENT OBJECTIVE:** Determine whether the session management policies of the RP allow sessions to extend past the lifetime of the assertion. **POTENTIAL ASSESSMENT METHODS AND OBJECTS**: **Test**: Log in to the RP with a short-lived assertion and ensure the session at the RP continues for some time after the assertion has expired, within the RP's re-authentication requirements.