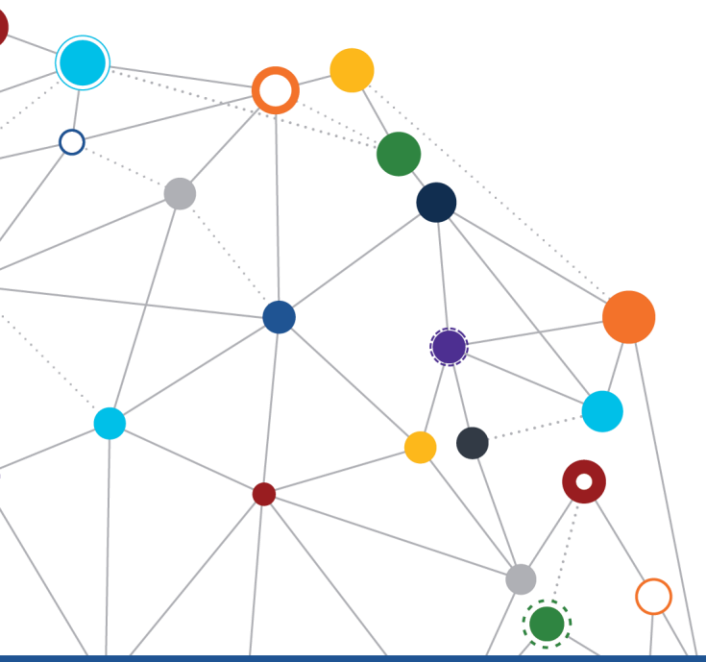
OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

Federation

March 2019 | Enterprise Program Management Office



VA | U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	3/4/2019	IAM Federation document approved

1 Context

The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) program to coordinate secure access to VA resources for both internal and external users. IAM services are guided by the Office of Management and Budget (OMB) M 11-11,[1] the Federal Information Processing Standard (FIPS) 200, the National Institute of Standards and Technology (NIST) Guidelines (800-63 and 800-53 per Appendix D), and the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance.

VA has two general populations of users who require access: (1) internal users include employees, contractors, trainees, and volunteers, and (2) external users, comprised of Veterans, beneficiaries, and health partners, including employees and contractors from other Government agencies. All require varying levels of access to interact with VA services.

2 Challenge

VA continues to innovate to make services more accessible for Veterans. To provide many services, the user must be identified and authenticated to be presented user-specific information, protect privacy, and prevent fraud. Per NIST 800-63C, "Federation allows a given credential service provider to provide authentication and (optionally) subscriber attributes to a number of separately-administered relying parties." Federation extends single sign-on by allowing users to "bring their own credentials." As the relying party, VA can accept credentials from an external credential service provider (CSP) to access VA services; however, the CSP must be approved.[2] Besides authentication, we need accurate information about the subscriber known as "assertions." Providing assertions that meet NIST 800-63C requirements is only sufficient to secure the federation transaction; and the ability to meet these requirements does not attest to the quality of the assertions themselves, as established earlier during identity proofing. Federation must be properly designed in context with all the other IAM services. The progression of how IAM services are engaged by users and system owners can be seen in Figure 1. This Enterprise Design Pattern (EDP) focuses on the area highlighted in red.

[1] Note that M 11-11 is a pending rescission. Refer to a draft OMB policy aligned with NIST 800-63 at https://policy.cio.gov/identity-draft/.

[2] For more information on CSP approval, refer to the *Identity Proofing* EDP at https://www.oit.va.gov/library/recurring/edp/index.cfm.

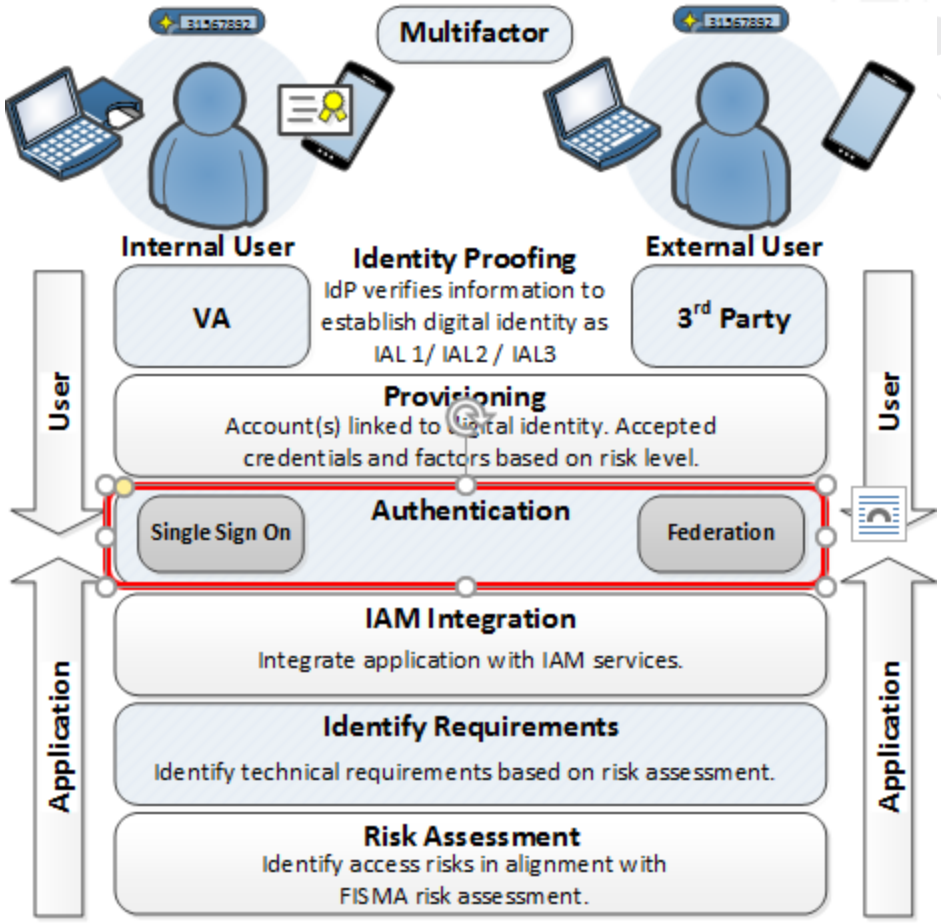


Figure 1: Overview of IAM Progression [3]

3 Approach

Federation is a process that facilitates the sharing of authentication and subscriber attribute information between networked systems that are not part of the same domain. In simple terms, it allows an external CSP, known as an identity provider (IdP), to authenticate a user and share information about that user to the relying party (RP). In this context, VA is the RP. The external IdP could be a commercial IdP or another Federal agency.

Several areas must be considered for federation to function. The IdP must:

- Be trusted by VA.

[3] Figure 1 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) EDP Team from information obtained from VA OIT IAM Subject Matter Experts (SMEs) and the National Institute of Standards and Technology (NIST) Publication 800-63A at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

- Use supported protocols.
- Perform identity proofing of the user at the appropriate risk level.
- Collect the attributes necessary to match the VA enterprise identity and make authorization decisions[4] to support the VA service that is accessed.

This document focuses on federation and requirements related to Federation Assurance Levels (FALs).

3.1 FAL Overview

The FAL describes the requirements for how assertions about a user are secured for a transaction. Table 2 describes the requirements for each FAL. At a minimum, all levels require keys for signing.

Table 2: FAL Requirements

Level	Description
FAL1	**Bearer assertion, signed by IdP.** FAL1 maps to the OpenID Connect (OIDC) Basic Client Profile or Security Assertion Markup Language (SAML) Web Single Sign-On (SSO) Artifact Binding Profile,[5] with no additional features.
FAL2	**Bearer assertion, signed by IdP and encrypted to RP.** FAL2 additionally requires that the assertion (e.g., the OpenID Connect ID Token or SAML Assertion) be encrypted to a public key representing the RP in question.
FAL3	**Holder of key assertion, signed by IdP and encrypted to RP.** FAL3 requires the subscriber to cryptographically prove possession of a key bound to the assertion (e.g., the use of a cryptographic authenticator), along with all requirements of FAL2. The additional key presented at FAL3 does not need to be the same key used by the subscriber to authenticate to the IdP.

The higher FAL meets all the requirements of the FAL(s) below it. It should be noted that the technical difficulty increases with each level. Projects that are required to use the Veteran-Focused Integration Process (VIP)[6] are subject to the VA Assessment and Authorization (A&A)

[4] Refer to the *IAM Authorization Planning* EDP at https://www.oit.va.gov/library/recurring/edp/.
[5] For more information on SAML profiles, refer to https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.
[6] Refer to the Veteran-Focused Integration Process (VIP) 3.2 Guide, December 2018, at https://vaww.vaco.portal.va.gov/sites/OIT/epmo/vip/Policy%20%20Guidance/VIP%20Guide%203.2.pdf.

Process,[7] which is based on the Risk Management Framework (RMF).[8] The associated risk assessment, completed as part of RMF, will result in a projected Federation Assurance Level (FAL), which will drive federation requirements.[9] As the FAL in use can be detected by the RP, VA must determine which FALs are acceptable for a given authentication transaction, and ensure that the transaction meets those requirements.

3.2 Establish a Federation

The following subsections describe how a federation can be established between VA and another party.

3.2.1 Federation Models

A federation is made up of the IdP members that provide authentication services and the RP members which consume those services. According to NIST, there are several types of models:

- Manual Registration – The IdP and RP manually exchange configuration information and establish a standard federation protocol.
- Dynamic Registration – The relationship between the members of the federation is negotiated at the time of the authentication event.
- Federation Authority – A third party, known as a federation authority, conducts some level of vetting of each potential federation member and provides approval.
- Proxied Federation - Communication between the IdP and the RP is intermediated by a proxy that prevents direct communication between the two parties. If a proxy is used, it must meet all the requirements for both the IdP and the RP.

In VA's model, all federation is established using manual registration. Although use of an IdP approved by the Trusted Framework Initiative (TFS)[10] may appear to follow the federation authority model, these IdPs must still be approved by VA and manually registered.

---

[7] Refer to the VIP Security Guide at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=27. The VIP Security Guide provides details about the A&A process and how it reflects an implementation of NIST guidance and VA security policies. For additional information on VA Assessment and Authorization, refer to https://www.va.gov/PROPATH/map_library/process_AAA_ext.pdf.

[8] Refer to the NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* at https://pages.nist.gov/800-63-3/sp800-63-3.html. In addition, the VA Handbook 6500, *Risk Management Framework for VA Information Systems*, can be referenced at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.

[9] Refer to the *IAM Risk Assessment* EDP at https://www.oit.va.gov/library/recurring/edp/.

[10] For more information on TFS, refer to *the Identity Proofing* EDP at https://www.oit.va.gov/library/recurring/edp/index.cfm.

3.2.2Assertion Presentation

Assertion presentation reviews how the assertion is communicated between the parties involved in the federation. Either back-channel or front-channel presentation may be used. A proxy may also be used; in this case, the audience would be restricted to the next hop (proxy or RP) in the flow. There are some general practices that apply to both models:

- The IdP must transmit only those attributes that were explicitly requested by the RP.
- Assertions must be validated by the RP to include the following elements: issuer, signature, time, and audience restriction.
- All communication between the subscriber, IdP, and RP must be protected in transit, using an authenticated protected channel.

Front-channel presentation is recommended because of the simplicity. No connectivity should be designed between the IdP and the RP. This reduces the complexity of the solution.

Back-channel presentation may be used when required, or if an improvement in latency is expected. Figure 2 provides an overview of the back-channel and front-channel models.

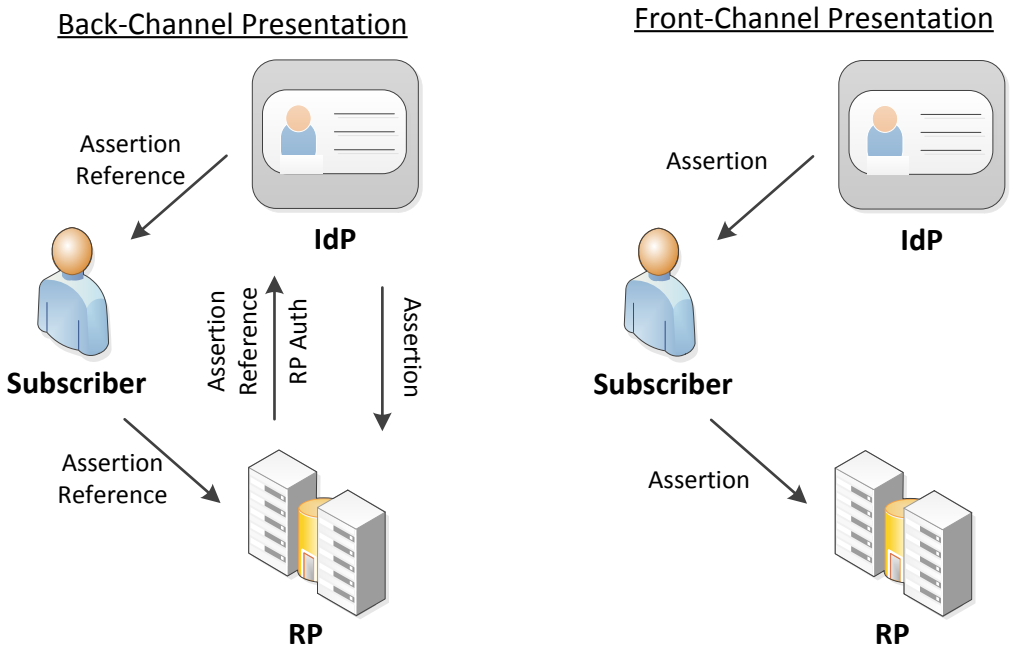


Figure 2: Federation Presentation Models[11]

[11] Figure 2 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) EDP Team from information obtained from VA OIT IAM Subject Matter Experts (SMEs).

- Back-Channel Presentation – Also known as synchronous bindings in Security Assertion Markup Language (SAML), the IdP sends the subscriber an assertion reference to present to the RP. The RP presents the assertion reference to the IdP and authenticates itself to be sent the full assertion. The assertion reference must be resistant to tampering and fabrication by an attacker. The strategy here is to reduce the ability to compromise assertions sent from the subscriber. Assertion references must:
    - be limited to one RP
    - be single use
    - not exceed the session expiration time
    - be presented by the RP to the IdP along with RP credentials
- Front-Channel Presentation – Also known as asynchronous bindings in SAML, the subscriber authenticates to the IdP that generates the assertion. The subscriber uses the assertion to authenticate to the RP. There are potential risks to all flows going through the subscriber. The following practices apply to front-channel models:
    - The RP must protect itself against assertion tampering. For example, the RP could block cross site scripting attempts.
    - The RP must require FAL2 or greater to protect the information in the assertion from disclosure to the browser or other parties.

3.2.3 Approval to Transmit Subscriber Information

NIST 800-63 states that federation of parties must not be interpreted as permission to pass information. RPs may establish whitelists of IdPs from which the RP will accept authentication and attributes without a runtime decision. RPs may also use blacklists; otherwise a runtime decision is made to allow the transaction. To simplify compliance in this area, VA must approve any IdP to be federated with VA. All IdPs that have not been approved must be blocked by default. This means that the subscriber may not authorize their own IdP since the selection is already limited to those approved by VA. VA approval of the IdP also ensures compliance with NIST 800-63 requirements.[12] VA must restrict the IdP based on the supported FAL. For example, the IdP should be blocked from submitting authentication attempts for a VA service that requires FAL3, if the IdP has only been approved at FAL2 and lower. Even if an IdP is approved by VA, assertions must not be transmitted between the federated parties, except for the following purposes:

- Identity proofing
- Authentication
- Attribute assertions
- To perform fraud mitigation related to an authentication event
- To comply with law or legal process

[12] For more information on IdP approval, refer to the *IAM Identity Proofing* EDP at https://www.oit.va.gov/library/recurring/edp/.

This is to protect the privacy of the subscriber. Through federation, the IdP could track the subscriber based on their connections to multiple RPs, beyond what it might normally be able to track. This requires the IdP to protect the privacy of the subscriber by restricting information sharing to the purposes above. For example, the RP would not be allowed to query the IdP for subscriber assertions to populate a new attribute being used across its user population.

3.3 Assertions

An assertion is a set of attribute values or attribute references associated with an authenticated subscriber. The assertion contains information about the subscriber established through identity proofing, as well as metadata and possibly other data the RP may use, such as expiration time. While the primary use of the assertion is to authenticate the user, it can support other use cases, such as authorization and personalization of services. It is recommended that an assertion only represent a single login event at the RP.

3.3.1 Assertion Metadata

All assertions must include the following metadata:

- Subject: the subscriber
- Issuer: An identifier for the IdP that issued the assertion.
- Audience: An identifier for the RP
- Issuance: A timestamp indicating when the IdP issued the assertion
- Expiration: A timestamp indicating when the assertion expires
- 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

Additional information may be collected to support various use cases. The RP must coordinate with the IdP in advance to determine how any attributes would be captured and presented.

3.3.2 Assertion Assurance Levels

It is recommended to have the IdP specify the Authenticator Assurance Level (AAL) for the authentication event being asserted and the Identity Assurance Level (IAL) for identity proofed attributes. If not specified, the RP may not assign any specific IAL or AAL to the assertion. This means the IdP must specify the AAL and IAL in the assertion where a specific assurance level is required to complete a transaction. This is required because any FAL used must meet the “Acceptable Combinations of AAL/IAL/FAL” policy defined by VA. Therefore, the AAL and IAL must also be defined. For more information, see the IAM Risk Assessment Enterprise Design Pattern.

3.3.3 Uniquely Identifying Subscribers

A RP must not treat subject identifiers as inherently globally unique. For example, there could be duplicate subject names across the IdP, even though it is unique within the individual IdP. The subject identifier is based on the namespace under the control of the IdP. VA IAM assigns the SecID to uniquely identify subjects where conflicts could exist with the subject identifier attribute. The SecID must be used to uniquely identify subscribers to avoid name conflicts.

3.4 Assertion Security

The integrity of the assertion must be protected to ensure that it is reliable for use. The primary means of protection is binding, connecting the assertion to the issuer or subscriber. The following section describes other protections to prevent impersonation.

3.4.1 Assertion Privacy

The RP must request attribute references, rather than full attribute values, whenever feasible. This minimizes exposure to the subscriber data. While this is conditional for the RP, based on the use case, it is mandatory for the IdP. The IdP must support attribute references.

3.4.2 Assertion Binding

Binding is used to connect a subscriber to an assertion, such as a name or other descriptor. When an assertion is presented to the RP by the IdP, the RP must determine if the binding is sufficient to connect to the subscriber; or if additional proof is required that the assertion is bound to the subscriber.

- Bearer Assertion – A bearer is an entity, and in this case, the IdP in possession of an assertion. The assertion could be intercepted and compromised; this is why each FAL has different protections.
    - FAL1 requires that the assertion be signed by the IdP. This demonstrates that the IdP possesses the assertion. Without this minimum level of security, the assertion cannot be trusted.
    - FAL2 requires signing by the IdP and encryption to the RP. This protects the assertion in transit.
- Holder-of-Key Assertion (HOK) - FAL3 requires Holder-of-Key (HOK) assertion. This method uses a reference key that represents the subscriber. The reference key is asserted and signed by the issuer. The subscriber authenticates to the IdP. As with other methods, the IdP presents the HOK assertion that references the key held by the subscriber. The subscriber proves possession of the key directly to the RP. This makes it difficult for an attacker. If an attacker steals an HOK assertion, the attacker must also need to steal the referenced key. The following applies to HOK:
    - The subscriber must prove possession of the key to the RP. If possession is not proven, the HOK assertion is considered a bearer assertion instead.
    - Unencrypted private or symmetric keys must not be included in HOK assertions.

- It is recommended to use a key that is distinct from any used by the subscriber to authenticate to the IdP.
- The RP may verify the claimant's possession of the key in conjunction with the IdP. In this case, the RP would also have the IdP verify the proof of possession of the key by the subscriber.

3.4.3Assertion Protection

In addition to binding and other types of protection that ensure the integrity of assertions, the following protections must be included:

- Key Management/Encryption – Approved cryptography must always be used. Additionally, government-operated IdPs asserting authentication at AAL2, and all IdPs asserting authentication at AAL3, must protect keys used for signing or encrypting those assertions with mechanisms validated at FIPS 140 Level 1 or higher.
- Assertion Identifier - Assertions must support unique identification by the target RP. This can be done by use of a nonce, identifier, or other means.
- Signed Assertion – All assertions must be digitally signed by the IdP and the signature validated by the RP. Keys can be symmetric or asymmetric. If symmetric, the RP must ensure that the IdP does not use the key for other RPs.
- Encrypted Assertion – Contents of the assertion must be encrypted by the IdP either using the RP public key or a symmetric key. If symmetric, the RP must ensure the IdP does not use the key for other RPs. If assertions are passed through third parties, such as a browser, the actual assertion must be encrypted.
- Audience Restriction - Assertions must use audience restriction techniques and be checked by the RP to verify it is the intended target. This prevents injection and replay of an assertion across RPs.
- Pairwise Pseudonymous Identifiers (PPID) – This combination of user and client is generated by the IdP as a unique identifier that represents the user for that particular client. The PPID protects the privacy of the subscriber across RPs, instead of providing a common identifier across all RPs. Note that correlation of attributes may still be possible to uniquely identify the subscriber by colluding RPs. Privacy policies are recommended to prohibit such correlation. There are some protections required when applying this practice.
    - General Requirements
        - The IdP must generate a different identifier for each RP. For example, VA could not share its SecID with multiple outside RPs.
        - If a proxied federation model is used, the proxy must not disclose the mapping between the PPID (between each IdP) 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.
    - PPID Generation

- The PPID must not contain identifying information about the subscriber and not be guessable by a party with some information about the subscriber.
- The identifiers must only be known and used by one pair of endpoints; however, an RP could request that the same identifier be used across RPs if:
    - The RPs have a demonstrable relationship that justifies an operational need for the correlation.
    - All RPs that share an identifier, consent to being correlated as such.
    - The RPs must conduct a privacy risk assessment to consider the privacy risks associated with requesting a common identifier.
    - The IdP must ensure that only intended RPs are correlated and RP impersonation is prevented.

4 Application of Practices

The following use case represents application of the federation practices described in this document.

4.1 Federation with an External IdP

4.1.1 Purpose

Updated Federal policy has been released with new requirements for federation. VA has many IT services which require external users to acquire and use credentials provided by an external Identity provider (IdP). An external IdP is required that is compliant with Federal policy and can scale to meet VA needs.

4.1.2 Assumptions

- A business justification exists for an external IdP for federation.
- VA IAM and the GSA FICAM website do not have a suitable and compliant IdP to meet business needs.
- A risk assessment has been completed to determine the appropriate AAL of the application that will use the federated authentication.
- The collection of any required assertions about the subscriber has been completed as part of planning for identity proofing.
- Once an IdP is determined to be technically viable and approved, a review of the procurement process is outside the scope of this use case.

4.1.3 Use Case Description

- The system owner has submitted the business case for a solution as a VIP Request (VIPR). The system requires integration with VA IAM for external user access.
- The system owner contacts the VA IAM service to identify available services. As part of the analysis, VA IAM determines that federation with an external IdP is required.
- The VA IAM does not have an approved IdP that is compliant with the updated Federal policy yet, and one is not approved through FICAM. A risk assessment is required to approve a new external IdP.
- The VA Access and Identity Management (AIM) Program Management Office (PMO) completes the risk assessment for a candidate IdP using vendor-supplied information, or available ATO documentation. The assessment validates the ability to meet technical requirements of the federation model to be used, and the minimum assurance level.
- The IdP is approved for use, the VA IAM registers the IdP, and the federation is established.

4.2 Key Practices

Table 3 highlights key practices identified in this EDP.

Table 3: Key Practices IAM Federation EDP

Category	Area	Description
Identity and Access Management	Federation	For FAL1, a bearer assertion must be signed by the Identity Provider (IdP).
Identity and Access Management	Federation	For FAL2, a bearer assertion must be signed by the (IdP and encrypted to the relying party (RP).
Identity and Access Management	Federation	For FAL3, Holder of Key (HOK) is required and must be signed by the IdP and encrypted to the RP.
Identity and Access Management	Federation	Proxied Federation: If a proxy is used, it must meet all the requirements for both the IdP and the RP.
Identity and Access Management	Federation	In VA's model, all federation is established using manual registration. Although use of an IdP approved by the Trusted Framework Initiative (TFS) may appear to follow the federation authority model, these IdPs must still be approved by VA and manually registered.
Identity and Access Management	Federation	The IdP must transmit only those attributes that were explicitly requested by the RP.
Identity and Access Management	Federation	Assertions must be validated by the RP to include the following elements: Issuer, signature, time, and audience restriction.

Category	Area	Description
Identity and Access Management	Federation	All communications between the subscriber, IdP, and the RP must be protected in transit using an authenticated protected channel.
Identity and Access Management	Federation	Back-channel presentation may be used when required, or if an improvement in latency is expected. Assertion references must be: • Limited to one RP. • Single use. • Limited to the session expiration time and must not exceed it. • Presented by the RP to the IdP, along with RP credentials.
Identity and Access Management	Federation	Front-channel presentation is recommended because of the simplicity supporting faster deployment. The following practices apply to front-channel models: • The RP must protect itself against assertion tampering. For example, the RP could block cross site scripting attempts. • The RP must require FAL2 or greater in order to protect the information in the assertion from disclosure to the browser, or other parties.
Identity and Access Management	Federation	VA must approve any IdP to be federated with VA; all IdPs that have not been approved must be blocked by default.
Identity and Access Management	Federation	VA must restrict the IdP on the basis of the supported FAL.
Identity and Access Management	Federation	Even if an IdP is approved by VA, assertions must not be transmitted between the federated parties, except for the following purposes: • Identity proofing • Authentication • Attribute assertions • To perform fraud mitigation related to an authentication event • To comply with law or legal process

Category	Area	Description
Identity and Access Management	Federation	All assertions must include the following metadata: • Subject: the subscriber • Issuer: An identifier for the IdP that issued the assertion • Audience: An identifier for the RP • Issuance: A timestamp indicating when the IdP issued the assertion • Expiration: A timestamp indicating when the assertion expires • Identifier: A value uniquely identifying this assertion that is used to prevent attackers from replaying prior assertions • Signature: Digital signature or message authentication code (MAC) for the entire assertion, including key identifier, or public key associated with the IdP • Authentication Time: A timestamp indicating when the IdP last verified the presence of the subscriber at the IdP
Identity and Access Management	Federation	The IdP must specify the AAL and (Identity Assurance Level) IAL in the assertion, where a specific assurance level is required to complete a transaction.
Identity and Access Management	Federation	The RP must not treat subject identifiers as inherently globally unique.
Identity and Access Management	Federation	The SecID must be used to uniquely identify subscribers to avoid name conflicts.
Identity and Access Management	Federation	The RP must request attribute references, rather than full attribute values, whenever feasible to minimize the subscriber data exposed.
Identity and Access Management	Federation	The IdP must support attribute references.
Identity and Access Management	Federation	When an assertion is presented to the RP by the IdP, the RP must determine if the binding is sufficient to connect to the subscriber; or if additional proof is required, determine if the assertion is bound to the subscriber.

Category	Area	Description
Identity and Access Management	Federation	Government-operated IdPs asserting authentication at AAL2, and all IdPs asserting authentication at AAL3, must protect keys that are used for signing, or encrypting those assertions with mechanisms that are validated at FIPS 140 Level 1 or higher.
Identity and Access Management	Federation	Assertions must support unique identification by the target RP.
Identity and Access Management	Federation	All assertions must be digitally signed by the IdP and the signature validated by the RP.
Identity and Access Management	Federation	Contents of the assertion must be encrypted by the IdP, either by using the RP public key or a symmetric key. If symmetric, the RP must ensure that the IdP does not use the key for other RPs. If assertions are passed through third parties, such as a browser, the actual assertion must be encrypted.
Identity and Access Management	Federation	Assertions must use audience restriction techniques and be checked by the RP to verify it is the intended target.
Identity and Access Management	Federation	If Pairwise Pseudonymous Identifiers (PPIDs) are used: • The IdP must generate a different identifier for each RP. • If a proxied federation model is used, the proxy must not disclose the mapping between the PPIDs (between each IdP) to a third party, or use the information for any purpose other than federated authentication, related fraud mitigation, compliance with the law or legal process, or in the case of a specific user request, for the information. • The PPIDs must not contain identifying information about the subscriber and not be guessable by a party with some information about the subscriber. • The identifiers must only be known and used by one pair of endpoints, unless (a) the RPs have a demonstrable relationship that justifies an operational need for the

Category	Area	Description
		correlation; (b) all RPs that share an identifier consent to being correlated as such; (c) the RPs conduct a privacy risk assessment to consider the privacy risks associated with requesting a common identifier; and (d) the IdP ensures that only intended RPs are correlated and RP impersonation is prevented.

5 Impacts

If risk management is not used to define the technical requirements for IAM components of VA solutions, the following risks are increased:

- FISMA non-compliance, contributing to a material weakness or other audit findings by external agencies with oversight
- Inadequate technical protections for sensitive data that may contribute to unauthorized access, data breach, or fraud

Appendix A: References

- DEA User Stories: https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/SitePages/Home.aspx
- FISMA User Stories: https://vaww.portal2.va.gov/sites/asd/AERB/FISMASecurityCompliance/SitePages/Home.aspx
- TRM: http://trm.oit.va.gov/
- NIST 800-63-3: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
- VA 6500.3: http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=733&FType=2
- VA 6510 (under revision): http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=823&FType=2

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.