ICAM

Identity, Credential,
& Access Management

Federal Identity, Credential, and Access Management
Trust Framework Solutions

Relying Party Guidance

For

Accepting Externally-Issued Credentials

Version 1.1.0

Questions?
Contact the FICAM TFS Program Manager at TFS.EAO@gsa.gov

Acknowledgements

This document was prepared by the Federation Interoperability Working Group (FIWG) of the Identity, Credential, and Access Management Subcommittee (ICAMSC) under the auspices of the Chief Information Officers (CIO) Council. This document provides guidance to agencies on the acceptance of externally-issued credentials. The ICAMSC wishes to thank members of the FIWG from the following agencies who reviewed drafts of this document and contributed to its development:

- Department of Agriculture
- Department of Homeland Security (DHS)
- DHS Homeland Security Information Network
- Department of Housing and Urban Development
- Department of Justice
- Department of State
- Department of Treasury
- Department of Veterans Affairs
- General Services Administration
- National Aeronautics and Space Administration
- National Institutes of Health
- National Science Foundation
- Program Manager for the Information Sharing Environment

Table of Contents

List of Figures

1. Purpose

The purpose of this document is to provide supplemental guidance and recommendations to the FICAM Roadmap[1] on implementing a capability for a citizen-facing government website and agency partner accessible application, referred to as a Relying Party (RP)[2] application, to accept third-party credentials. The *Relying Party Guidance for Accepting Externally-Issued Credentials* is a living document that evolves as policy and technology changes. This document is intended to assist business owners and technical resources responsible for the management and maintenance of the RP application.

In support of the purpose, this document was written to:

- Provide detailed guidance to an RP owner around current mandates and compliance requirements;
- Identify best practices, lessons learned, and approaches to implementing the acceptance of federated credentials; and
- Explore scenarios in support of the acceptance of third-party credentials.

1.1. Audience

This guideline is intended for:

- **Agency Program Mangers and Implementers**, who are seeking to integrate the ability to accept externally issued credentials into their applications.
- **Security and Privacy Practitioners**, who recommend, design, build or provide solutions that meet U.S. Federal Government requirements

1.2. Usage

1. Read the *Trust Framework Solutions Overview* to understand the background, authorities and components of the FICAM TFS Program
2. Read the *Relying Party Guidance for Accepting Externally Issued Credentials* to understand how to leverage federated identity technologies.
3. Read the *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services* to understand the requirements that providers need to satisfy in order to offer identity services to the U.S. Federal Government
4. Read the *Identity Scheme and Protocol Profile Adoption Process* to understand how protocol profiles are created, adopted and used by the government to ensure that the RP application and the CSP communicate in a confident, secure, interoperable and reliable manner.

[1] FICAM Roadmap

[2] As defined in the FICAM Roadmap, Appendix B Glossary.

1.3. Scope

This document is the *Relying Party Guidance for Accepting Externally-Issued Credentials*, and its scope is limited to analysis, considerations, and recommendations related to implementing a capability for citizen-facing government websites and agency partner accessible applications to accept FICAM-approved third-party credentials from entities external to the Federal Government. This includes:

- Externally-facing, internet accessible, government applications operating at all levels of assurance supported by the Trust Framework Solutions (TFS) Initiative; and
- Externally-issued FICAM-approved credentials.

The following items fall outside the scope of this document:

- Applications accessible only to internal agency users;
- Authorization via assertion (e.g., Attribute Based Access Control);[3]
- Personal Identity Verification (PIV) and PIV Interoperable (PIV-I) credentials;
- Implementation guidance on accepting credentials that are not FICAM-approved; and
- Vendor specific details.

Additionally, this document does not directly include content that is discussed in detail in the FICAM Roadmap.[4] Where relevant, this document includes references to Chapter 12 of the FICAM Roadmap and expands on the information provided at a high level, as listed in Figure 1.

Section	Topic Area
Federation Overview	• Introduces the common need for agencies to provide access for non-federal users • Discusses why an agency should consider federation • Introduces the most common trust topologies[5] that are used to describe an agency's relationship with external parties
Federal Trust Framework	• Provides an overview of the mechanisms that exist to support acceptance of externally-issued credentials, based on the credential type • Explains how these elements support cross-organizational trust
Provisioning External Users	• Provides guidance on a number of different scenarios, processes, and mechanisms to enable agencies to provision accounts for external users
Federated Access Using Third-Party Credentials	• Provides guidance for leveraging third-party credentials; including determining acceptable credentials, working with Credential Service Providers (CSPs), and implementing a capability to accept credentials issued outside of the agency

Figure 1: Federation Topics

[3] Authorization will be addressed in a future version of this document. For additional information, refer to Access Control and Attribute Governance Working Group.

[4] Unless otherwise noted, please refer to the FICAM Roadmap as the authoritative source for more detailed discussions omitted from this document.

[5] Trust topologies are information exchange approaches that an agency may choose in order to accommodate the wide range of mission and business reasons behind federation.

This page is intentionally left blank

2. Background

The FICAM Trust Framework Solutions (TFS) is the federated identity framework for the U.S. federal government. It includes guidance, processes and supporting infrastructure to enable secure and streamlined citizen and business facing online service delivery.

The *Trust Framework Solutions Overview* document provides a holistic overview of the components of the TFS which consists of:

- *Trust Framework Provider Adoption Process (TFPAP) for All Levels of Assurance*
- *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services*
- *Identity Scheme and Protocol Profile Adoption Process*
- *Relying Party Guidance for Accepting Externally Issued Credentials*
- E-Government Trust Services Certificate Authority (EGTS CA)
- E-Government Trust Services Metadata Services (EGTS Metadata Services)

The FICAM Roadmap also introduces an agency-level initiative, Initiative 9: *Implement Federated Identity Capability*, requiring agencies to reduce the issuance of local agency credentials for external users and instead leverage trusted third-party credentials.

This Relying Party Guidance for Accepting Externally-Issued Credentials provides agencies with architecture and implementation guidance that addresses existing Identity, Credential, and Access Management (ICAM) objectives and supports the goals for accepting externally-issued credentials. It provides business and technology owners with specific approaches and direction related to:

- Creating a business case through aligning an organization's business and technology strategy in order to securely conduct online transactions with individuals outside of the organization;
- Commonly used solution architecture models that can be leveraged to support the acceptance of third-party credentials, based upon clearly defined characteristics of each model;
- Leveraging Credential Service Providers (CSP) approved under the FICAM Trust Framework Solutions Program as directed by OMB policy; and
- The recommended processes and technologies to accept third-party credentials while ensuring security, privacy, and liability needs are upheld when choosing a CSP.

3. Federation Overview

When the Federal Government performs business transactions with entities outside of the Federal Government, it is necessary to take the proper measures to ensure that the mechanisms are in place for such transactions to be conducted in a secure and effective manner. As such, a federation[6] environment allows one organization to trust credentials created and issued by an

[6] As defined in the FICAM Roadmap, Appendix B Glossary.

outside organization. This environment enables a user of one domain to seamlessly and securely access the systems of another domain without the need for and burden of creating an additional credential. Leveraging federation to accept and trust third-party credentials offers multiple benefits to an RP, including:

- **Reduced Management.** Managing the user's credential is delegated to the CSP, thereby decreasing administrative burden.
- **Increased User Traffic.** Expanding the credentials that can be accepted opens the application to more users and can allow for more business to be conducted on a daily basis.
- **Enhanced User Experience.** Leveraging an existing credential alleviates the need for the user to be issued an additional username/password for the application. This ease of use characteristic is important in retaining users to continue to use the application without the burden of managing a new username/password combination. In turn, an RP may realize reduced help desk calls.
- **Meeting Agency Goals.** Accepting the use of third-party credentials helps agencies meet business objectives and achieve compliance with government-wide mandates such as NSTIC, the FICAM Roadmap, and the E-Government Act.

Additional benefits realized when an RP accepts externally-issued credentials in accordance with the guidance provided in this document include cost savings, enhanced privacy protections, increased confidence in user identity, streamlined revocation of access, and increased security. These benefits are discussed in depth in Section 12.1.1 of the FICAM Roadmap.[7]

3.1. Federation Process

Federation requires at least three parties, one party that has an application which it wishes to allow access to (i.e., the RP), another party that has issued credentials to the target users of the application (i.e., the CSP), and the user who needs access to the RP application. A fourth party, the attribute provider, may be involved in a federation where additional information about a user is required. The attribute provider acts as an independent entity that maintains a set of attributes about the user. For a particular transaction, the attribute provider and the CSP can be the same entity. These parties are defined[8] as follows:

- **Credential Service Provider (CSP).** Entity that establishes an individual's identity and links the identity to a credential. CSPs validate the identity of the individual using the credential and pass along verification of the individual's identity to an RP.
- **Attribute Provider.** Entity that holds additional attributes about a user. The attribute provider can provide attributes to the CSP or the RP during a transaction. An attribute provider can either be an independent entity or be the CSP itself. Within the scope of this section, the CSP and attribute provider are shown as the same entity.
- **Relying Party (RP).** Entity that requests and/or receives information about the identity of an individual or an authentication assertion from another party such as a CSP. The

[7] FICAM Roadmap

[8] As defined in the FICAM Roadmap, Appendix B Glossary.

requestor is referred to as an RP, since the requestor relies upon information provided from the external source to authenticate an identity.

- **User.** Entity that establishes an authenticated session with a CSP by providing his/her identity and token for verification. The user can provide more than one token for a higher level of assurance.

The roles and responsibilities of a CSP and RP are detailed in Section 3.2 and Section 3.3 respectively.

Terminology

Assertion – a statement from which an entity verifies a user's identity, such as an enterprise authentication service, to a Relying Party that contains identity information about a user. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.[9]

As noted above, federation typically involves externalizing authentication of the credential to the CSP and leveraging assertions to communicate between the CSP and RP (as discussed in Section 3.1.1). In the case of PKI credentials, however, the RP will commonly perform the authentication event and validate the PKI credential itself due to the path discovery and validation process for PKI. This is referred to as direct-PKI authentication and it is discussed further in Section 3.1.2.

3.1.1. Federated Authentication by a Credential Service Provider

In federated authentication, the RP will route the user to an external CSP to validate his/her credentials. Once the CSP authenticates the user, the CSP will send an assertion to the RP indicating that the user has successfully been authenticated. Figure 2 depicts the process associated with a basic federated authentication transaction[10] between the RP and CSP.

[9] FICAM profiles define how a protocol must be implemented to meet federal requirements. See Section 4.2 for more details.

[10] See Appendix A for more detailed scenarios and process steps associated with the federated authentication process outlined in Figure 2.

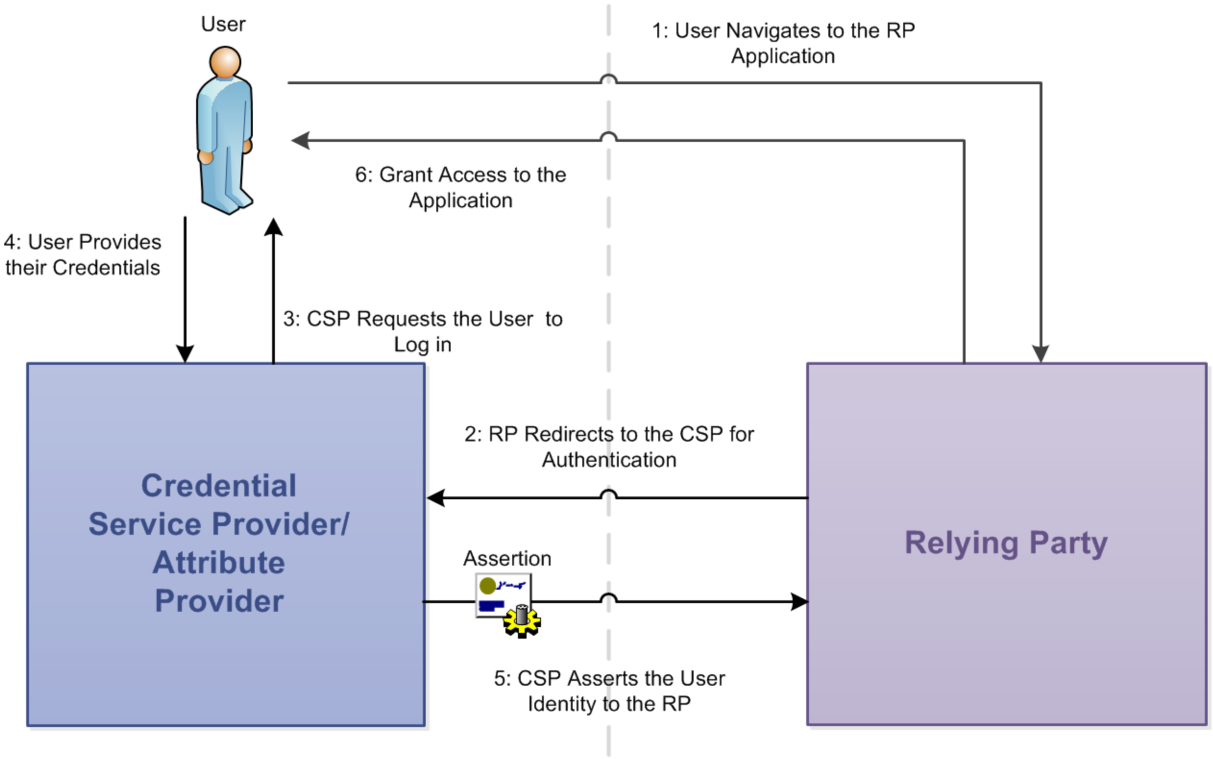

User
1: User Navigates to the RP Application
6: Grant Access to the Application
4: User Provides their Credentials
3: CSP Requests the User to Log in
Credential Service Provider/ Attribute Provider
2: RP Redirects to the CSP for Authentication
Relying Party
Assertion
5: CSP Asserts the User Identity to the RP

Figure 2: Relying Party to Credential Service Provider Federated Authentication Process

As illustrated in Figure 2 above, the RP to CSP federated authentication process includes the following steps:

1. The user initiates the flow of events by navigating directly to the RP application site.
2. The RP application presents a list of acceptable CSPs, and the user selects to log into the RP application with a CSP credential he/she possesses. The RP application then redirects the user to the selected CSP.
3. The CSP prompts the user to enter his/her credential.
4. The user enters his/her credential and is successfully authenticated with the CSP.
5. The CSP then redirects the user back to the RP application and sends an assertion to the application verifying the user's identity.
6. The RP application validates and parses the assertion to verify and grant access to the user.

In step 5 of the federated authentication process, the CSP sends an assertion to the RP. In the assertion, the CSP can also provide attributes about the user who authenticated. In this way, the CSP also acts as an attribute provider. In some federation scenarios, there may be an independent attribute provider who can provide additional attributes to the CSP or the RP. In step 6 of the federated authentication process, as part of granting access to the user, the RP is responsible for determining the specific privileges assigned to the user and enforcing the access control policies for the application (i.e., authorization). Since authorization is solely the responsibility of the RP and occurs outside of the basic authentication process, it is not covered further in this document.

In addition to the approach shown in Figure 2, a user can also navigate directly to the CSP to initiate the federated authentication process. In this method, the CSP authenticates the user and then redirects him/her to the RP application to complete the process. There currently have not been any government-wide CSP-initiated use cases identified for accepting externally-issued credentials; therefore it is not expanded upon further in this document.

For examples of current federations within the Federal Government, please see the case studies in Appendix B and Appendix C.

3.1.2. Direct Authentication with a PKI Credential

Direct authentication involves a user that presents a credential directly to an RP for validation. In terms of externally-issued credentials, this authentication model is used for PKI credentials issued by a certificate authority (CA) that is cross-certified with the Federal Bridge Certification Authority (FBCA). A user may possess an externally-issued PKI credential issued by a federal agency (e.g., PIV card) or by an external CSP (e.g., PIV-I card). This process is shown in Figure 3.

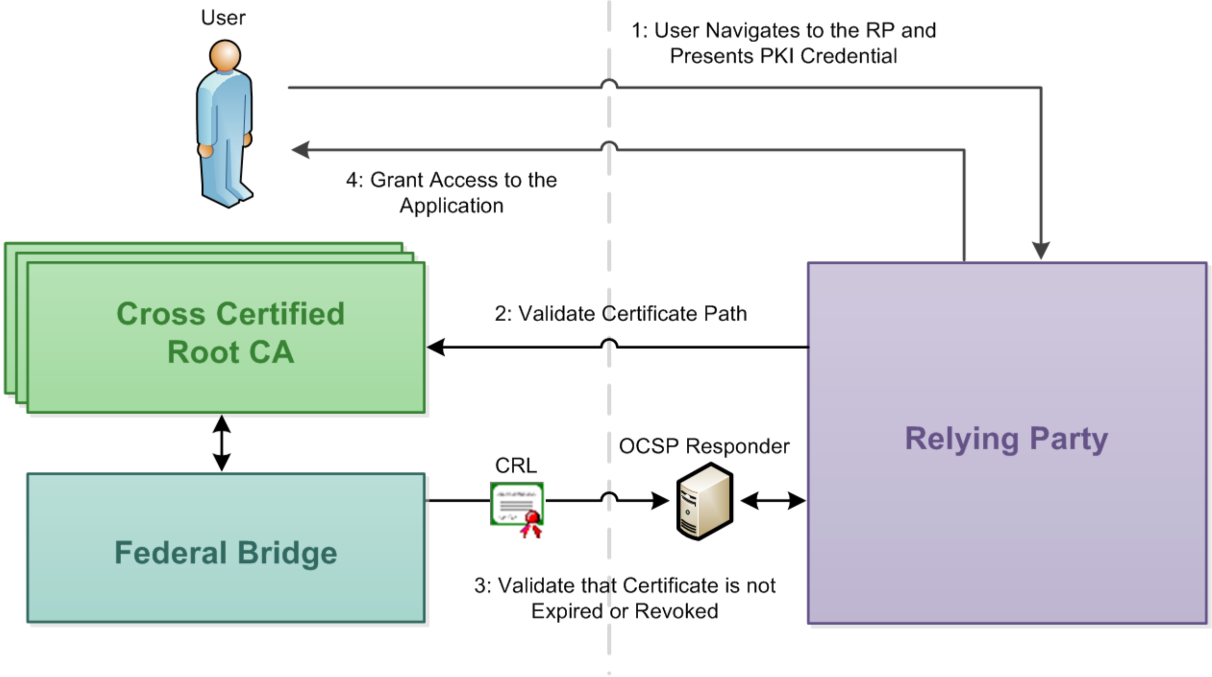

User
1: User Navigates to the RP and Presents PKI Credential
4: Grant Access to the Application
Cross Certified Root CA
2: Validate Certificate Path
Relying Party
OCSP Responder
CRL
Federal Bridge
3: Validate that Certificate is not Expired or Revoked

Figure 3: Direct Authentication using a PKI Credential

As illustrated in Figure 3, direct authentication to an RP includes the following steps:

1. The user initiates the flow of events by navigating directly to the RP application site and presenting their PKI credential for authentication.
2. The RP validates the certificate path from the PKI credential to the root CA.
3. The RP validates that the certificate is not expired or revoked by leveraging either an Online Certificate Status Protocol (OCSP) responder or a Certificate Revocation List (CRL).
4. The RP application grants access to the user.

As part of granting access to the user in step 4, the RP is responsible for determining the specific privileges assigned to the user and enforcing the access control policies for the application (i.e., authorization).

A PKI credential that is issued by a CA that is cross-certified by the FBCA is a valid externally-issued credential, and as such should be accepted by an RP. However, this document focuses on the brokered authentication model where the authentication event is externalized to a CSP as shown in Section 3.1.1. For additional information on PKI validation and the FBCA, please reference the Federal PKI webpage.[11]

3.2. Credential Service Provider

During a federated access transaction, the CSP validates the identity of the individual using the credential and passes along verification of the individual's identity to the RP through an assertion. Based on these activities, the responsibilities ascribed to a CSP include:

- **Manage the credential life cycle.** The CSP's responsibility with respect to the life cycle of a credential begins with identity proofing, which is used to vet and verify the information that is used to establish a user's identity. This duty extends through issuance, maintenance, revocation, and possibly reissuance. These activities alleviate the RP of the burden of managing the life cycle of the user's credential.
- **Maintain the security of the information collected about the user during the identity proofing process.** Due to the nature of credential issuance, the CSP may collect Personally Identifiable Information (PII) about the users to whom it issues credentials. It is important that a CSP properly secure the information and only disclose it when required by policies, mandates, and applicable laws. Privacy considerations and implications are further discussed in Federal ICAM Privacy Guidance for Trust Framework Assessors and Auditors.[12]
- **Authenticate users on behalf of the RP.** As illustrated in Figure 2, a CSP verifies[13] a user at the request of an RP within the federation. When a user is successfully authenticated with a CSP, the CSP asserts the user's identity and only the required attributes to the RP.[14]

Privacy Tip

A Relying Party (RP) should only request attributes that it requires for the transaction. Additionally, the Credential Service Provider should collect and/or transmit only those identity attributes that were specifically requested or required by the RP.

[11] For additional information please see the Federal PKI webpage.

[12] Federal ICAM Privacy Guidance for Trust Framework Assessors and Auditors, Version 1.0, June 29, 2011, [FICAM Privacy Guidance for Trust Framework Assessors and Auditors].

[13] As defined in SP 800-63, The Verifier verifies the Claimant's identity by verifying the Claimant's possession and control of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status. The CSP serves as the Verifier in Figure 2.

[14] It should be noted that a user can have multiple credentials for different CSPs; therefore, RPs should take into consideration how such a situation should be managed, or if it should be managed at all. Section 7.2.2.1 provides further guidance.

3.3. Relying Party

In a federated access transaction, the RP receives information from a CSP through an assertion and uses the information as input to the access control decision process. Based on these activities, the responsibilities ascribed to an RP include:

- **Establishing policies for accessing a protected resource.** When an RP is determining the criteria for accessing a specific resource, it should evaluate existing laws, government policies, and agency-specific policies for accessing that resource. If policies regarding who is allowed to access a resource do not exist, then they should be determined and enforced.
- **Managing the risk associated with operating the application.** The RP should conduct appropriate risk assessments in accordance with relevant policy and implement risk management techniques as necessary.[15]
- **Determining the level of assurance for the protected resource.** The RP should determine the appropriate level of assurance required for the application. This level of assurance dictates which CSP credentials are acceptable for transactions with the RP application.
- **Protecting the privacy and security of a user's PII.** An agency should consider the privacy and security of a user's PII during the planning (i.e., design-time) and operating (i.e., run-time) phases of the application. During planning, the RP should determine the minimal amount of information that the application requires for each user to operate correctly. During run-time, the RP should only request required information, supporting the privacy-enhancing principle of data minimization.

Privacy Tip

Privacy Offices maintain an inventory of the agency's systems and applications that house individual identity data called the System of Records Notice (SORN). During planning,[16] agencies can review the SORNs to see where each data element is collected and stored.

- **Validating each identity assertion.** In order to communicate with the CSP, the RP needs to authenticate the CSP and validate the integrity of the assertion. To validate the identity assertion, the RP should consult the specification of the protocol being used, as the mechanism used to authenticate the CSP and validate the assertion is different for each protocol. For example, Security Assertion Markup Language (SAML) leverages metadata acquired from the CSP in order to validate the assertion during run-time. SAML and other protocols are further discussed in Section 4.2.
- **Authorizing a user to leverage a protected resource.** After receiving an assertion and verifying its validity, the RP should determine which functions within the application the user is allowed access to. The RP will review policies that surround the application and make a determination on the requirements to access different functions within the application. The RP, however, compares the assertion and attributes provided to the access control policy during run-time and makes an access control decision.

[15] See Section 5.2 for further guidance on conducting risk assessments and managing risk.

[16] For additional guidance on planning, see Chapter 5.

This page is intentionally left blank

4. Establishing Trust in a Federated Environment

Today's need to conduct business with organizations outside of the Federal Government has created the requirement for trust relationships between government agencies and third-party credential providers to securely carry out business. In the case of an RP, the ability to accept identity attributes and credentials from external sources requires that a trust relationship be in place.

As an RP prepares to accept third-party credentials, the trustworthiness of the CSP is a critical component. The CSP needs to have a mechanism in place to protect the confidentiality, integrity, and availability of the information that it provides to the RP in order for an RP to accept externally-issued credentials. To facilitate the establishment of trust with a CSP, the Federal Government has established the Trust Framework Solutions Program, which outlines an approach and processes for leveraging industry-based credentials that citizens already have for other purposes. This chapter outlines key concepts within the Trust Framework Solutions Program, discussed in the following sections:

- **Trust Framework Solutions Overview.** This section provides an overview of the Trust Framework Solutions Program, which establishes the basis of trust when accepting credentials issued by third-party CSPs.
- **Approved Identity Schemes and Protocol Profiles.** This section discusses overlaying federal requirements on industry standard protocols to allow for interoperability between a CSP and an RP in a trusted manner.
- **Non-FICAM-Approved Credentials.** This section discusses the implications of accepting credentials from a CSP that has not been approved by a Trust Framework Provider (TFP) and a comparison of a FICAM-approved CSP and non-approved CSP.

4.1. Trust Framework Solutions Overview

As previously discussed, the Trust Framework Solutions Program establishes the basis of trust for an RP when it is externalizing its authentication to an approved CSP. Figure 4 shows how this trust is established under the Trust Framework Solutions Program.

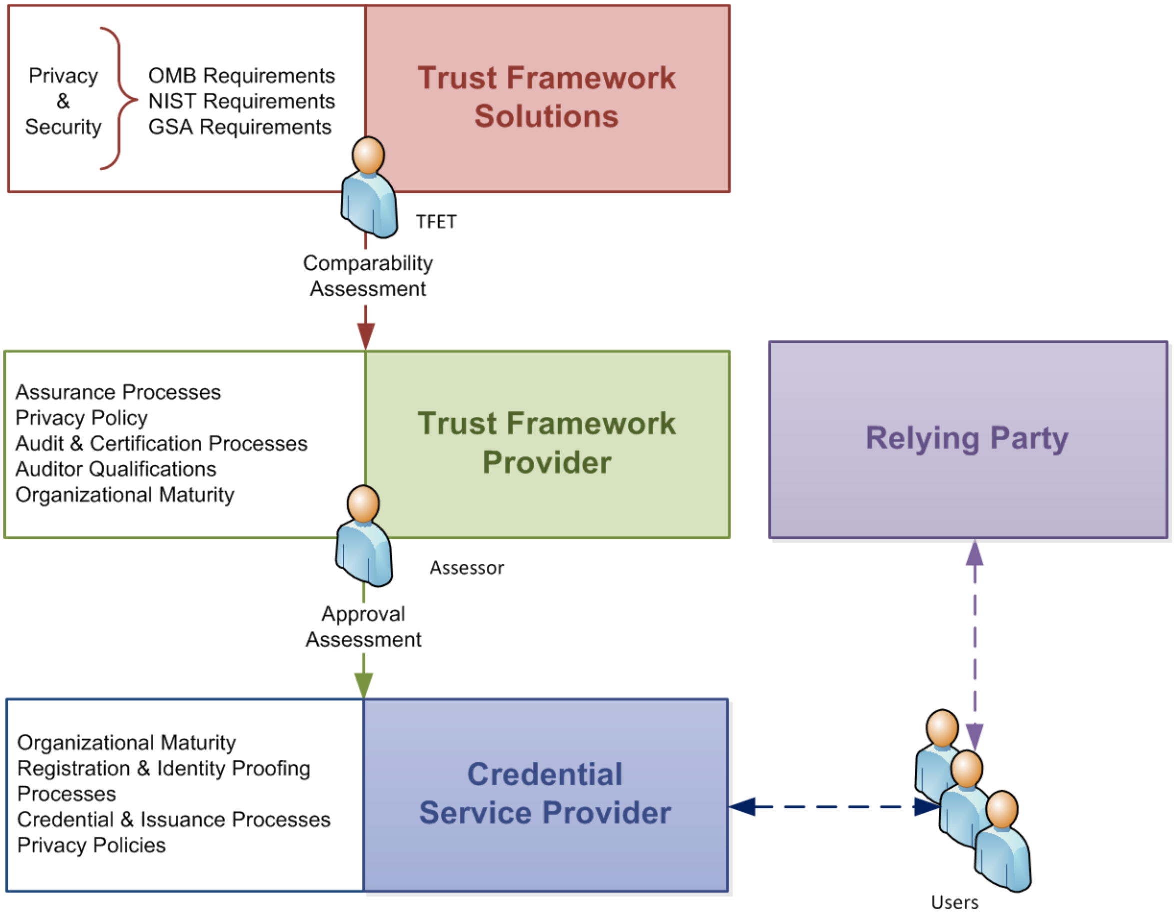


Figure 4: Trust Framework Solutions Entity Relationships

As illustrated in Figure 4, the relationships that span between the Trust Framework Solutions, TFPs, and CSPs are interconnected. Within the Trust Framework Solutions Program, the *Trust Framework Provider Adoption Process (TFPAP)* is used to assess existing, industry-based Trust Frameworks and approve them as TFPs. TFPs in turn define the processes for assessing CSP credentialing processes against federal requirements for issuance, privacy, and auditing as codified by OMB, NIST, and the General Services Administration (GSA).

Once a TFP has been approved by FICAM TFS via the TFPAP, it then has the ability to assess and certify various identity services such as Token Managers (TMs) which provide the authentication functions, Identity Managers (IMs) which provide the identity proofing and attribute management functions, and Credential Service Providers (CSPs) who provide a full service capability that combines authentication, identity proofing and the secure binding of token(s) to identity.

The identity services that have been qualified by a FICAM Approved TFP as meeting TFPAP requirements have the option of applying to the FICAM TFS Program to request approval for the authority to offer their services to the U.S. Federal Government using the processes documented in the TFS *Authority To Offer Services (ATOS) for FICAM TFS Approved Identity Services*.

Use of a CSP approved under the Trust Framework Solutions Program allows an RP to be confident that the CSP provides the following characteristics:

- Trust, particularly that the CSP has the appropriate processes for identity proofing and credential lifecycle management;
- Robust and reliable technical interoperability between endpoints through the use of FICAM profiles;
- The expected level of assurance; and
- The required level of privacy protection.

At the time in which the CSP has been approved, an RP can choose to allow users to use credentials issued by that CSP. The RP will benefit from enhanced confidence that the CSP has appropriately vetted the identities that it will assert to the RP. It is important for the RP to only allow credentials at the appropriate level of assurance. Considerations for selecting a CSP are provided in Section 7.1.1 of this document.

4.2. Approved Identity Schemes and Protocol Profiles

In addition to the mechanisms put in place by the TFPAP, the *Identity Scheme and Protocol Profile Adoption Process*[17] assists in enhancing the security and privacy at the transaction level through creating FICAM Profiles for use by RPs and CSPs. The exchange of messages between an RP and a CSP pertain primarily to the exchange of an identity assertion[18] and are standardized via FICAM Profiles. These assertions include verification of a user's identity and the transmission of attributes about the individual accessing the RP application.

Terminology

Identity Scheme and Protocol Profile Adoption Process – a standard process for adopting and leveraging open standards, protocols, and technologies for government-wide implementation. This process does not alter the existing standard, maintaining the interoperability with industry. Instead, it incorporates best practices to ensure interoperability, security, and privacy that is compliant with the Federal Government.

The FICAM Profiles do not alter the underlying industry standard upon which it is based, but identify how the specification language is implemented for technical interoperability of government applications. Proper use of a FICAM Profile assists an RP in its implementation by:

- Meeting federal standards, regulations, and laws;
- Minimizing risk to the Federal Government;
- Maximizing interoperability; and
- Providing users with a consistent context or user experience at a Federal Government site.

Using the *Identity Scheme and Protocol Profile Adoption Process*, the government can assess the efficacy of specific subsets of identity management standards for federal purposes. This helps the RP application and the CSP communicate in a confident, secure, and reliable manner.[19] Two

[17] A more detailed discussion of the Identity Scheme Adoption Process can be found in Section 12.2.2.2 of the FICAM Roadmap.

[18] As defined in the FICAM Roadmap, Appendix B Glossary.

[19] M-04-04

current examples of profiles that are applicable to the federal space include OpenID and SAML.[20] These profiles are discussed below.

Characteristic	OpenID	SAML
Description	A standards-based protocol that facilitates exchange of messages between endpoints for the purpose of exchanging an identity assertion that includes authentication and attribute information.[21]	An Extensible Markup Language (XML)-based protocol for exchanging authentication and authorization data between endpoints. Security Assertion Markup Language (SAML) uses security tokens containing assertions to pass information about an individual between a Credential Service Provider (CSP) and a web service.[22]
Industry Background	• Open Source roots • OpenID Foundation serves as steward • Broad Commercial Off-The-Shelf (COTS) support • More than 1 billion OpenID enabled accounts • More than 40,000 websites support OpenID	• OASIS SAML 2.0 Web Browser single sign-on (SSO) Profile • Based on the e-government profile developed through Liberty Alliance • Broad COTS support • Leveraged by the Federal Government previously
FICAM Profile	• Profile based on OpenID 2.0 • Requires Secure Socket Layer/Transport Layer Security (SSL/TLS) on endpoints • Requires Directed Identity Approach • Requires pair-wise unique pseudonymous identifiers • Requires short-lived association handles • Level of Assurance (LOA) 1	• Requires e-government profile • Requires encryption of Personally Identifiable Information (PII) • Level of Assurance (LOA) 1, 2, and 3 identity authentication • Holder-of-key assertions for binding keys or other attributes to an identity at LOA 4

Figure 5: OpenID and SAML Profiles Overview

For a more detailed discussion around the identity scheme adoption process, OpenID, and SAML please refer to Section 12.2.2.2 of the FICAM Roadmap.[23]

The *Identity Scheme and Protocol Profile Adoption Process* also provides a mechanism to protect a user's privacy. Privacy is contextual in nature, and data often moves across organizational and system boundaries where shared context may not exist. This makes it difficult to develop rigorous, repeatable processes to protect user privacy. While challenging, building privacy protective mechanisms into government systems is crucial to attracting and maintaining users. NIST DRAFT Special Publication (SP) 800-130[24] has defined the following three characteristics of privacy:

[20] For a current list FICAM Profiles, see Adopted Profiles & Identity Schemes.

[21] OpenID 2.0 Profile, Version 1.0.1, November 18, 2009, [OpenID].

[22] Security Assertion Markup Language (SAML) 2.0 Web Browser Single Sign-on (SSO) Profile, Version 1.0.2, December 16, 2011, [SAML].

[23] FICAM Roadmap

[24] SP 800-130, DRAFT A Framework for Designing Cryptographic Key Management Systems, NIST, April 2012 [800-130].

- **Anonymity**. Assures that public data cannot be related to the owner.
- **Unlinkability**. Assures that two or more related events in an information processing system cannot be related to each other.
- **Unobservability**. Assures that an observer is unable to identify or infer the identities of the parties involved in a transaction.

These characteristics are consistent with the TFPAP activity tracking criteria, where CSPs must not disclose information on end user activities with the government. Additionally, there is a focus on not being able to trace a user's interactions across multiple RPs. FICAM profiles help preserve user privacy in this manner through the implementation of the Private Personal Identifier (PPID). A PPID corresponds to a user and is unique for every user-RP pair. The use of PPIDs can mitigate the loss of anonymity and loss of unlinkability by uniquely identifying an end user at each RP they visit. While the issue of unobservability remains, developers continue to seek ways to limit the visibility into citizen information and where a user authenticates. Additionally, since the PPID persists for a given RP, the RP can implement single sign on (SSO) across applications within the RP agency. However, since the PPID is different across multiple RPs, users will not have SSO across agencies.

FAQ

What is a Private Personal Identifier (PPID)? Does the FICAM Profile Require its Use?

A PPID is a pairwise pseudonym identifier used to uniquely identify an end user to each Relying Party (RP) he/she visits. It assists in enhancing the privacy protection of a user's Personally Identifiable Information (PII) and preserves a user's privacy across multiple RPs. Yes, both the Security Assertion Markup Language (SAML) and OpenID FICAM Profiles require the use of PPID. This complies with federal privacy requirements for not tracking the activity of a user across the government.

4.3. Non-FICAM-Approved Credentials

As previously mentioned, the OMB memo for Accepting Externally-Issued Credentials requires agencies to only accept externally-issued credentials issued in accordance with NIST guidelines and Federal CIO Council processes.[25] Leveraging third-party credentials provides great benefits to government agencies; however, circumstances may arise where an RP does not find an approved CSP for its community. It is important that an RP be aware of the costs and issues associated with accepting external credentials that are not FICAM-approved. Figure 6 describes the differences between implementing external credentials that are not approved by a TFP and those that are.

[25] Memorandum for Chief Information Officers of Executive Departments and Agencies: Requirements for Accepting Externally-Issued Identity Credentials, Office of Management and Budget (OMB), October 6, 2011.

Consideration	FICAM-Approved CSP	Non-Approved CSP
Design and Implementation Effort	• FICAM Profiles define secure, confidential communication protocols • Standards-based • Credential Service Provider (CSP) already vetted and approved at specified levels of assurance • Addresses federal security and privacy considerations	• Continued monitoring and auditing required to ensure CSP is meeting requirements • Additional design required to negotiate secure, confidential communication protocol • May not be standards-based • Relying Party (RP) needs to independently verify the identity proofing and credential level of assurance of the CSP • Additional time, resources, and/or budget likely required to define, implement and test protocol with the CSP
Scalability and Federation	• Trust Framework Provider performs onboarding of new CSPs resulting in additional available CSPs for RP to leverage	• Limited support for protocols and standards • Access to a limited number of CSPs • Each additional CSP will likely require another "one off" design and implementation
FISMA Security Controls	• Helps address Federal Information Security Management Act (FISMA) controls related to identity proofing and credential issuance • Proper CSP-related controls provided by Trust Framework Provider Adoption Process (TFPAP)	• Additional controls required for ensuring that the external CSP is performing identity proofing and credential lifecycle management in accordance with policy • More difficult to obtain Authority to Operate (ATO) • Additional risks may need to be added to Plan of Actions and Milestones
Technical Interoperability	• Technical interoperability (e.g., security and confidentiality) is facilitated by extensive FICAM Lab research, analysis, testing of protocol standards for use in the FICAM Profiles	• Technical interoperability errors may exist due to new design work, differences in interpretation of the protocol specification and insufficient testing
Government-wide Mandates/ Objectives	• Complies with government mandates and objectives	• Inconsistent with government-wide objectives
FICAM Lab	• Can leverage FICAM Lab subject matter experts and services to help resolve challenges faced during implementation of third-party credentials	• Unable to leverage FICAM Lab

Figure 6: Comparison of FICAM-Approved and Non-Approved CSP

The use of non-approved CSPs is against policy; therefore, an RP should not leverage a non-approved CSP. Additionally, accepting external credentials that are not FICAM-approved requires that an agency independently assess the CSP to ensure that it meets security, privacy, and policy requirements. The agency will likely incur an increased effort and cost for managing the relationship, on-boarding, and technical implementation associated with using the CSP.

Implementation Tip

If a Relying Party (RP) identifies a non-FICAM-approved Credential Service Provider (CSP) that they want to use, the RP can recommend that the CSP go through the approval process of a Trust Framework Provider (TFP). This will benefit the RP by having the CSP audited and approved, benefit the CSP by providing it with a broader user base, and benefit the government by expanding the network of CSPs available for use.

This page is intentionally left blank

5. Federation Planning

Understanding the benefits and drivers for accepting third-party credentials and successfully leveraging the Trust Framework Solutions Program provides the necessary foundation for an RP to begin its planning period. The planning period is used to build a business case and gather relevant details for the applications being updated to accept third-party credentials. This chapter provides a discussion around the planning considerations and best practices to help the RP implement a solution to accept third-party credentials. These sections include:

- **Identifying Business Considerations.** This section provides guidance for an RP to create a business case that takes into account which of the agency's applications are required or may benefit from modification to accept third-party credentials and the associated cost of doing so.
- **Understanding the RP Environment.** This section provides guidance for an RP to understand details about its application through reviewing and conducting various assessments.
- **Mitigating Residual Risk.** This section provides guidance to an RP on addressing the residual risk remaining after addressing eAuthentication risks.
- **Determining Applicability to Security and Privacy Controls.** This section provides guidance on the security and privacy controls for an RP application that are affected by implementing a federation solution.

The considerations discussed within this chapter are for operational, externally-facing applications. As such, the applications should have existing assessments completed that can be referenced as a starting point for understanding the RP environment. Once the RP has completed the planning activities described in this section, the RP will have enough information to select a solution architecture and begin implementation.

5.1. Identifying Business Considerations

A successful federation implementation is one that takes an agency's mission and business needs into consideration and supports an agency's processes for interfacing with its customers. When there are many externally facing applications, the cost savings are amplified thereby increasing the benefits of accepting of third-party credentials. The RP can use this information to strengthen its business case and gain leadership approval. To build the business case, the RP will need to document the costs and benefits of accepting third-party credentials.[26] This can be accomplished by taking the following steps:

- **Estimate upfront cost of implementation.** The number of applications that require the acceptance of third-party credentials will dictate the solution architecture[27] that should be used. This will in turn determine what existing infrastructure can be reused, the new infrastructure that needs to be put in place, and the cost of implementation and maintenance.

[26] Further details about developing a business case and the acquisition and capital planning process can be found in Chapter 6 of the FICAM Roadmap.

[27] Solution architecture options are discussed further in Section 6.2.

- **Estimate application integration costs.** The cost should be calculated based on the integration effort per application. The application integration effort will depend on the complexity of the application, how easily its authentication method can be modified, and the ability to link third-party credentials to RP accounts.
- **Estimate ongoing costs.** In addition to the implementation cost, other life cycle costs should also be considered including management, governance, operations, and maintenance of the system. If a shared service provider is used, such as the federation broker described in Section 6.2.3, then the RP should also account for ongoing service charges.
- **Estimate benefits.** After the costs are known, the benefits and return on investment (ROI) can be calculated for the reduction of the need to identity proof and manage credentials.
- **Create a phased approach.** A phased and prioritized approach should be used to split activities into achievable milestones and demonstrate incremental benefits. In this manner, the agency can achieve tangible results in each phase of the program.

5.2. Understanding the RP Environment

Understanding the RP environment prior to enabling federation is another aspect for federation planning. It is necessary for the RP to determine if there will be any impacts to assurance level or existing privacy considerations through externalizing identity proofing and credential lifecycle management. Key steps for evaluating the RP environment include:

- **Gather existing documentation.** As part of designing and deploying an RP application, a variety of assessments related to security, authentication, and privacy should be conducted, including the ICAM maturity model[28] if one has been completed, Federal Information Processing Standard (FIPS) 199[29] security categorization, eAuthentication risk assessment,[30] Privacy Impact Assessment (PIA), and System of Records Notice (SORN).
- **Review and analyze documentation.** Existing documentation should be reviewed to understand the current state of the RP application. After reviewing the assessments, the RP should conduct a gap analysis between the current and target state. This will provide the RP with the detailed requirements and design that it will need to implement a federation capability.
- **Update documentation (if necessary).** The RP will need to determine if the documents it gathered require updates. While the FIPS 199 assessment may be reused, an eAuthentication risk assessment, PIA, and SORN should be updated to reflect the target state, which includes accepting externally-issued credentials, as necessary. To carry out these tasks, the RP should familiarize itself with applicable stakeholders within the agency, which can be found in Section 6.1.2 of the FICAM Roadmap.

[28] ICAM Maturity Model, Version 1.0, August 26, 2011.

[29] FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, February 2004, [FIPS 199].

[30] The Electronic Risk and Requirements Assessment (e-RA) is a sample tool that has been developed to help agencies conduct an eAuthentication risk assessment.

FAQ

Can the results of my FIPS 199 assessment and eAuthentication risk assessment be different?
Yes, the eAuthentication assurance levels are not directly related to the system security categories defined by FIPS 199. The FIPS 199 assessment determines the security categorization of the application based on the impact of a breach of confidentiality, integrity, and availability to the application. The eAuthentication risk assessment is focused on the risk associated with the authentication event.

- **Conduct application assessment.**[31] Once the agency has determined the risks and privacy impacts that affect its application, the next step is to conduct a deep dive review of the application in preparation for implementation. This review consists of understanding the application security model in order to paint a comprehensive picture of the application's current state and future state to assist in performing a gap analysis. The information gained from this assessment will be used by the application development team within the agency to create a detailed design, describing how changes will be implemented to the application in order to accept third-party credentials.

Figure 7 provides additional details related to the different assessments that should be gathered and reviewed by the RP and highlights specific actions that should be taken by the RP when pursuing a federation solution.

Assessment	Description	RP Actions
FIPS 199	FIPS 199 defines potential impacts on organizations or individuals should there be a breach of security. The results of a breach are categorized as low, moderate, or high.	• Identify existing FIPS 199 assessment and security category. • Determine if accepting third-party credentials is classified as a major change[32] to the application's security posture and if so determine if a new FIPS 199 is required. • Determine if the system's security controls specified by NIST SP 800-53 need to be changed.
eAuthentication Risk Assessment	An eAuthentication risk assessment focuses on the risk associated with false/positive authentication. The results of the assessment determine the recommended strength of the authentication requirements expressed as Levels of Assurance (LOA) 1 to 4.	• Conduct (or re-assess) eAuthentication risk assessment for each application that is being modified to accept third-party credentials and determine assurance level for that application. • Enforce the use of a credential that matches or exceeds that level of assurance for the given application. • Select a Credential Service Provider (CSP) that meets or exceeds the level of assurance of the application; this is discussed further in Section 7.1.1. • Identify if any residual risk remains and determine whether to accept the risk or select and implement compensating controls.

[31] A sample application assessment questionnaire can be found in Appendix D.

[32] What constitutes a major change is at the discretion of the agency. In addition, the agency may choose to conduct a new FIPS 199 assessment regardless of the change being classified as major or not.

Assessment	Description	RP Actions
Privacy Impact Assessment (PIA)	A PIA is an analysis of how information is handled to: • Ensure that it complies with legal, regulatory, and policy requirements regarding privacy (e.g., Privacy Act of 1974); • Determine the risks and effects of collecting, maintaining, and disseminating such information; and • Examine and evaluate protections and alternative processes for handling information to mitigate privacy risk.	• Identify the attributes that the Relying Party (RP) needs about a user. The RP can use these attributes to link the user's CSP identity to his/her RP account. Account linking is discussed in detail in Section 7.2.2. • Identify which attributes are necessary to complete the transaction. If the attributes are not necessary, reduce the set of attributes in order to be in compliance with the minimalism[33] principle. • Identify which of the attributes are Personally Identifiable Information (PII). This is especially important when handling information about public citizens. • Determine requirements to protect the PII.
System of Records Notice (SORN)	A SORN is used to ensure that agencies are not creating an unnecessary burden on individuals; nor collecting or using information for purposes that are not consistent with the intent of the application.	• Determine the legal authority for collecting the information. • Identify how collected information is shared outside the agency.

Figure 7: Assessments Required for Planning

5.3. Mitigating Residual Risk

As described in Figure 7, the RP will need to understand its environment through analyzing and conducting several assessments. Specifically, the eAuthentication risk assessment is used by the RP to understand and identify the risks associated with the RP application. The results of the eAuthentication risk assessment are mapped to an assurance level from M-04-04, which in turn helps inform the RP on the level of assurance requirements that need to be met when selecting a CSP. However, at times there may be a mismatch between the risk level of the application and the available level of assurance from the CSP. After conducting a risk and impact evaluation, the RP may determine that its assurance requirement falls in between two levels of assurance.

[33] FICAM Privacy Guidance for Trust Framework Assessors and Auditors

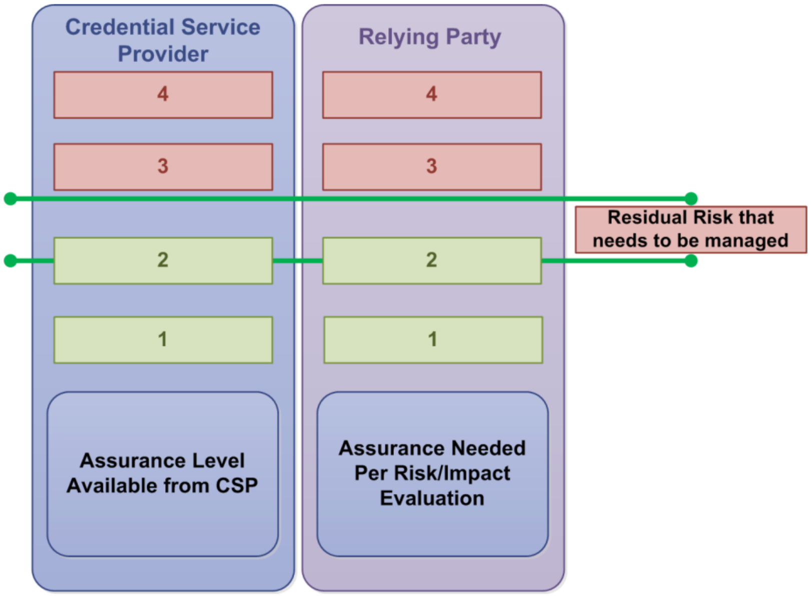

Credential Service Provider
Relying Party
4
4
3
3
Residual Risk that needs to be managed
2
2
1
1
Assurance Level Available from CSP
Assurance Needed Per Risk/Impact Evaluation

Figure 8: Residual Risk Identified During eAuthentication Risk Assessment

In Figure 8, the risk posed to the RP is deemed higher than LOA 2 but does not yet meet the criteria of LOA 3. In this case, if the RP chooses to leverage a CSP approved at LOA 2, there will be an amount of residual risk remaining. The RP can choose one of the following approaches for managing the risk:

- **Avoid.** The RP is not willing to take on the residual risk associated with the lower assurance credential; therefore the RP could either choose not to accept externally-issued credentials or choose to leverage a higher assurance credential from a third-party.[34]
- **Mitigate.** The RP chooses to proceed with using the lower level assurance credential and implements compensating controls to address the residual risk.
- **Accept.** The RP deems that the residual risk is acceptable per agency guidelines and risk tolerance and formally approves operating with the known risk.

In order to mitigate the risk, the RP can select and implement compensating controls for the application. Compensating controls for this type of risk would fall into the following categories:

- **Compensating controls for authentication.** Compensating controls for authentication may come in the form of additional authentication measures (e.g., shared secrets, multi-token e-authentication schemes, out-of-band confirmation)[35] or identity validation measures. For example, the RP may choose to require the user to authenticate with multiple form factors and conduct additional vetting of the user after receiving the assertion from a CSP.
- **Compensating controls for a layered security program.** eAuthentication provides an assessment of the risks associated with the authentication event. When the RP cannot fully mitigate the risk of authentication, it can implement layered security. The strength

[34] It is assumed that the RP application is already established and therefore the RP cannot avoid the risk by choosing not to offer the service online.

[35] Table 7 of SP 800-63 provides a description of multi-token E-Authentication schemes.

of layered security lies in using different controls at different stages of a transaction and the ability to compensate for weakness in one control with the strength of a different control. Layering different controls to activate at different times during a transaction process can create a robust, multi-dimensional program to strengthen overall security.

5.3.1. Compensating Controls for Authentication[36]

Compensating controls allow for flexibility in the design of an authentication solution. This flexibility is required if the authentication process is subject to business or usability constraints or if the authentication process has to adapt to a changing threat environment (i.e., new threat agents or new vulnerabilities).

Compensating controls also have drawbacks. Because they are customized, they increase overall costs and process complexity. Increased complexity can lead to a more frustrating user experience and to additional maintenance. So, while attractive in the short run, compensating controls can be problematic in the long run. The controls used may become ineffective as threat agents adapt, or they may introduce privacy risks and impose additional security constraints if the controls use application-specific information or PII. If compensating controls are to be considered in an authentication solution, the benefits and drawbacks should be carefully weighed against one another.

When selecting compensating controls, the RP should verify that the compensating controls are:

- Appropriate to the application, service, or transaction context; and
- Dynamic and easily adaptive, particularly in a highly fluid threat environment (e.g., a public-facing Internet service).

Additionally, an RP should verify that compensating controls do not:

- Place an unnecessary burden on the user being authenticated (otherwise, the user might abandon the service);
- Use personal or application-specific information that might raise privacy concerns. If such information is used, its use should be strictly limited to a specific application, service or transaction. The use of this information may result in unforeseen vulnerabilities or open a new threat vector and thereby be counterproductive; and
- Escalate the assurance level of a credential for use elsewhere (e.g., enable a Level 2 credential to be relied on as a Level 3 credential).

Electronic authentication technologies are evolving quickly due to rapidly changing technology and the constantly changing cyber-threat landscape. An RP should be aware of the latest best practices and standards that are being developed to address these threats and should carefully weigh the benefits and drawbacks against its risk posture to determine if compensating controls for authenticating users is the appropriate method to mitigate their residual risk.

5.3.2. Compensating Controls for a Layered Security Program

An RP implementing compensating controls as part of a layered security program should select and implement controls in accordance to the Risk Management Framework (RMF).[37] Figure 9

[36] Guideline on Defining Authentication Requirements, Treasury Board of Canada Secretariat, Government of Canada.

provides an overview of the risk assessment process, the RMF, and the intersection between the two.

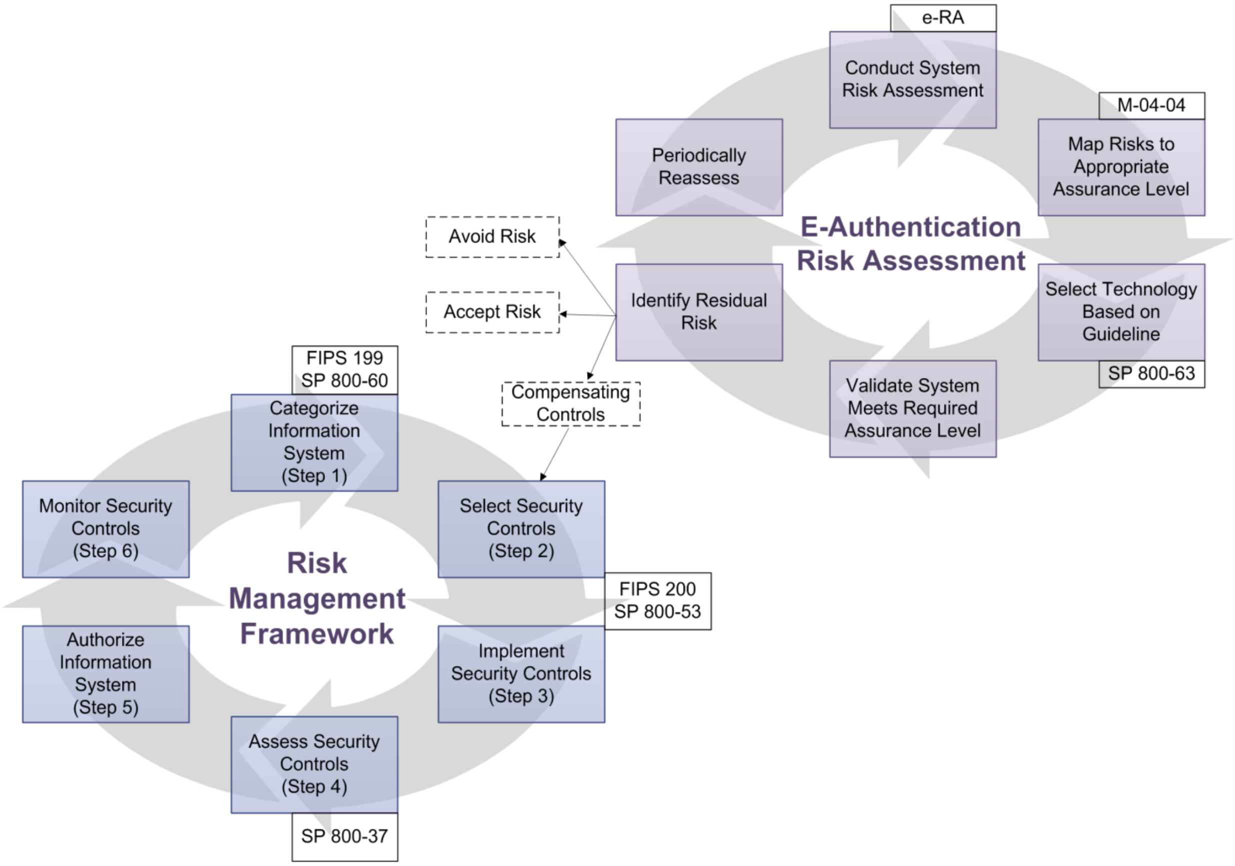

e-RA
Conduct System Risk Assessment
M-04-04
Map Risks to Appropriate Assurance Level
Periodically Reassess
E-Authentication Risk Assessment
Avoid Risk
Accept Risk
Identify Residual Risk
Select Technology Based on Guideline
SP 800-63
Validate System Meets Required Assurance Level
Compensating Controls
FIPS 199
SP 800-60
Categorize Information System (Step 1)
Monitor Security Controls (Step 6)
Select Security Controls (Step 2)
Risk Management Framework
FIPS 200
SP 800-53
Authorize Information System (Step 5)
Implement Security Controls (Step 3)
Assess Security Controls (Step 4)
SP 800-37

Figure 9: eAuthentication Risk Assessment and RMF Cycles

The RMF, shown on the left side of Figure 9, requires the RP to select and implement a set of security controls. These controls range from a full set of technology, security, and privacy controls.

The authentication process may exist within a larger context of security control mechanisms that mitigate risks as part of the RMF. Although a transaction may require a higher assurance level, the residual risk may be mitigated by other security controls that are not related to authentication, but that are within the system or are downstream from the authentication process. Additionally, other safeguards should be designed to capture and contain the downstream effects of an authentication error. For example, if an authentication error results in unauthorized access, the resulting access should be compartmentalized to a subset of low-risk transactions or non-sensitive information.

The controls that are specific to federation are discussed in Section 5.4. Beyond the normal set of controls, the RP may also choose to implement a set of compensating controls to mitigate the residual risk identified in the eAuthentication risk assessment. Compensating controls are an

[37] The Risk Management Framework is discussed in SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, NIST, February 2010, [SP 800-37].

additional set of controls selected out of the broader control families described in NIST SP 800-53.[38] Once all compensating controls have been implemented, an agency should evaluate to determine if there is any remaining residual risk and repeat the risk management steps as needed.

5.4. Determining Applicability to Security and Privacy Controls

As a next step, the RP should determine if it needs to modify the security and privacy controls associated with its application. For an existing application, it is expected that the security controls were selected and implemented as part of the security requirements under Federal Information Security Management Act (FISMA) and the RMF. Implementation of a federation solution, however, is likely to affect the existing controls because of the changes associated with managing and granting access to users. For example, any security controls related to the RP's management and direct validation of user credentials would need to be updated to reflect the shift of responsibility for the activities associated with authentication to an external CSP.

The assessments described in Section 5.2 provide an input into the controls that an agency needs to implement. These controls are based on SP 800-53,[39] which defines a set of control families that are specific to security and privacy.[40] While it is important for the RP to review and implement all of the control families, the scope of this document is the control families that are impacted by third-party credentials. These include:

- **Identification and Authentication (IA).** These controls are in place to ensure that users and devices are properly authenticated prior to allowing access to an Information Technology (IT) resource.
- **Access Control (AC).** These controls ensure that proper restrictions are in place to limit access to authorized users with a need to know.

If the RP needs to implement compensating controls for a layered security program, it will need to implement controls in addition to these two control families. The RP will need to determine what other control families in SP 800-53 are applicable depending on the risks posed to the application and the security posture of the agency.

Based on the assessments completed, the RP will need to assess the impact of the changes made to the application on its security controls. The RP should compare these impacts to its existing controls to determine if it needs to add new controls or modify existing controls. The RP should review each control and perform an assessment to determine how to appropriately meet the control. A tool to help the agency conduct this impact analysis is called the Security Impact Analysis (SIA). This tool provides an orderly process for analyzing the proposed changes to the information system and analyzing the potential effects on the overall security posture of the information system. A sample SIA is provided in Appendix E as a reference.

[38] SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, NIST, February 2012, [SP 800-53].

[39] SP 800-53

[40] Privacy controls can be found in Appendix J of SP 800-53.

Lesson Learned

Implementing an agency-wide ICAM solution provides a centralized mechanism to implement security controls, increasing efficiency and eliminating the need to implement controls separately for each application. The National Aeronautics and Space Administration (NASA) has processes in place for an application owner to integrate his/her application with the NASA ICAM solution, thereby allowing the application owner to inherit the controls implemented by the ICAM solution.

This page is intentionally left blank

6. Federation Architecture

The elements required to implement federation varies from one agency to another. Choosing the correct approach to accepting third-party credentials is highly dependent on the number/type of applications and infrastructure that an agency currently has in place. This chapter provides guidance for an RP as it prepares to implement a solution architecture that best fits the agency/RP needs in order to accept third-party credentials. The sections in this chapter include:

- **Evaluating Existing Infrastructure and Services.** This section discusses the possible states of an agency's ICAM infrastructure and how the infrastructure and services can be leveraged to provide a basis for federation.
- **Developing the Solution Architecture.** This section details three reference architectures that can be used when accepting third-party credentials. It also provides a list of considerations around each approach.
- **Selecting the Optimal Architecture.** This section discusses considerations that can be leveraged to help an agency choose its optimal architecture approach.

6.1. Evaluating Existing Infrastructure and Services

As each RP looks to accept third-party credentials, the requirements inherent to each application may vary, which in turn may affect the architecture that it chooses to leverage. An RP needs to look to its agency to determine if a complete or partial ICAM solution already exists. The ICAM team or Program Management Office (PMO) can provide the RP with guidance on the agency's policies and methodology for ICAM. For example, if the agency has a complete ICAM solution and application owners are required to integrate with it, the ICAM PMO will be able to provide details to the RP on how this integration will work and what the RP needs to do. If no ICAM solution exists, the PMO may be able to provide the RP with agency policies and standards in addition to resources to assist the RP with planning and design. The RP should work with the ICAM PMO[41] to complete the actions described in Figure 10.

Agency ICAM Solution Status	Description	Considerations
No Existing ICAM Solution	An agency has no centralized identity and access management system. Each application provides its own access control function, and maintains information about its users in a disconnected data store.	• Align with the agency's requirements. • Determine if the agency would benefit from an enterprise federation solution or if the Relying Party (RP) should implement a stand-alone solution.
ICAM Solution Partially Meets Requirements	An agency has a centralized identity and access management system; however, it does not provide federation capability that meets the requirements of the RP.	• Determine specific requirements that the RP has that are not met by the existing ICAM solution. • Determine if the existing solution can be modified to meet the requirements of the RP at the enterprise level. If not, the ICAM Program Management Office may be able to assist the RP in implementing a stand-alone federation solution.

[41] If an ICAM PMO does not exist, the RP should identify the appropriate governance body to assist with technology decisions and acquisitions.

Agency ICAM Solution Status	Description	Considerations
ICAM Solution Fully Meets Requirements	An agency has a centralized identity and access management system with which many of the applications integrate. In addition, this solution provides federation capability that meets the requirements of the RP.	- Integrate with the existing enterprise federation solution.

Figure 10: Impact of ICAM Solutions on Federation Deployment

After the RP has determined the current state of its agency's ICAM solution, it is in a position to leverage this information to determine the appropriate architecture approach.

6.2. Developing the Solution Architecture

An agency should develop the appropriate federation solution architecture based on the requirements, number of applications, and infrastructure in place. Solution architectures for accepting third-party credentials include stand-alone, enterprise, and federation broker. Each of these architectures has a common set of requirements (i.e., the ability to integrate with a CSP, parse an assertion, and link RP accounts); however, there are variations to how those requirements are implemented. Within this section, each of these solution architectures are discussed in further detail including a high-level overview, key considerations, and the requirements associated with each model.

6.2.1. Stand-Alone Application Architecture

The stand-alone application architecture directly enables the application to receive identity assertions from a CSP. In this architecture, applications require integration effort on an individual basis. That is, if two applications require third-party credentials from the same CSP, the applications will need to integrate with that CSP separately. This architecture is illustrated in Figure 11.

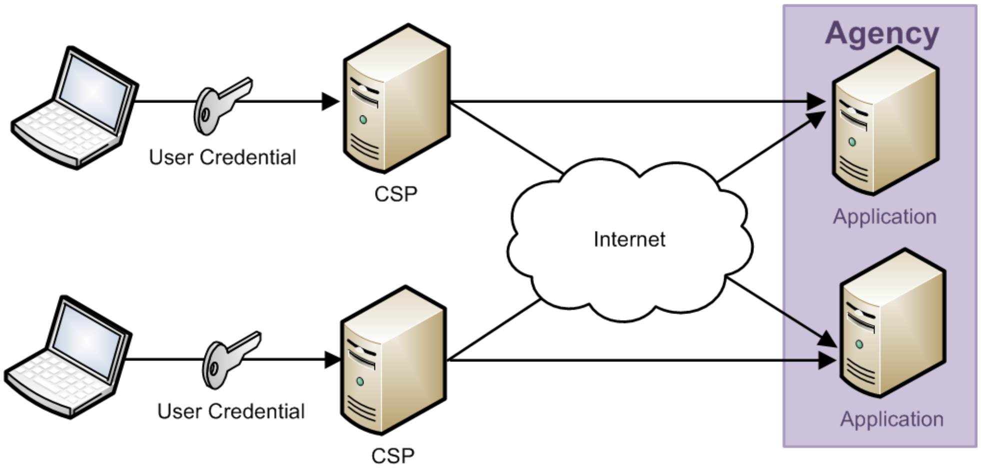


Figure 11: Solution Architecture 1 Stand-Alone Application

The stand-alone application architecture works by individually enabling federation support for each application, creating a many-to-many relationship between the CSPs and applications. The application will need to be modified so that it can communicate with the CSP and accept third-party credentials. This can be accomplished through application specific plug-ins or custom code. These plug-ins and custom code allow the application to parse the assertion sent by the CSP. Whenever a CSP is added, modified, or removed, the plug-ins and/or custom code of each application may need to be updated.

Figure 12 provides an overview of how the architecture requirements for a stand-alone federation approach are implemented.

Architecture Requirement	Implementation Location	Number of Implementations
CSP Discovery Page	Application	Once per application
CSP Integration	Application	Once per CSP/application combination
Assertion Parsing	Application	Once per application
Assertion Translation	N/A	N/A
Authorization Enforcement	Application	Once per application
Account Provisioning and Linking	Application	Once per application

Figure 12: Solution Architecture 1 Requirements

This architecture approach does not provide scalability for agencies with many applications, as the effort required compounds with the addition of each application. The considerations for an RP implementing this architecture include:

- Requiring per application updates to support onboarding, modification, and off-boarding of CSPs;
- Requiring ongoing maintenance efforts to upkeep each application's federation capability. Since the federation capability is a customization to the application, the agency will need to retain the knowledge and skillset to maintain the application;
- Customizing the application may affect future updates and patches released by the vendor of the application;
- Providing a low effort method to pilot the acceptance of third-party credentials before implementing a more robust solution; and
- Requiring minimal implementation effort when an agency has a limited number of applications.[42]

6.2.2. Enterprise Federation Architecture

The enterprise solution architecture employs a centralized federation server for the agency.[43] In this architecture, the centralized federation server establishes a connection with various CSPs. This integration enables applications within the agency to accept third-party credentials from those CSPs. The CSP integration is a one-time activity per CSP, as opposed to the stand-alone application architecture, where each application has to separately integrate with each CSP. This architecture is shown in Figure 13.

[42] Stand-Alone Application Deployment may not be the optimal solution if an agency has more than several applications it wishes to enable the acceptance of third-party credentials. The initial expenditure and maintenance cost of this approach increases in a linear fashion with each application that is federation enabled. For an agency that will enable more than three or four applications, another approach is recommended to reduce overall cost.

[43] A federation server, as defined in this document, is the same as a federated access manager, which is defined in the Section 11.2.2.5 of the FICAM Roadmap.

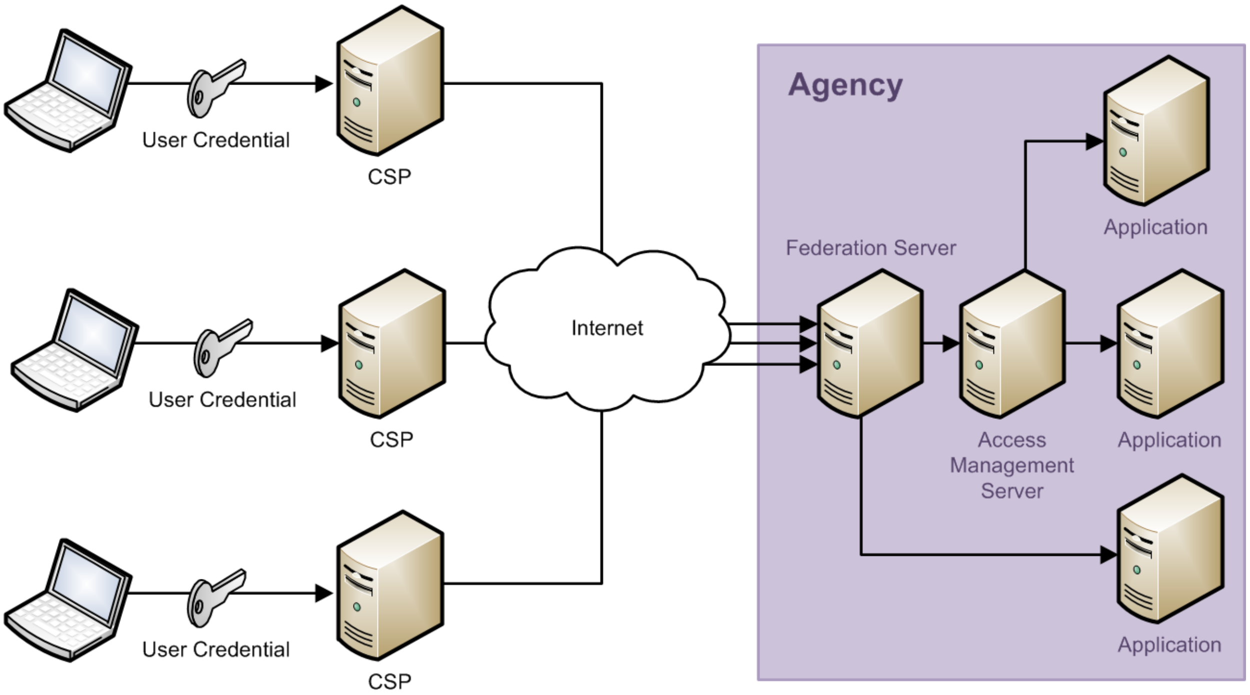


Figure 13: Solution Architecture 2 Enterprise Federation Architecture

The enterprise federation architecture works by connecting each CSP to a centralized federation server, thus creating a one-to-many relationship between the CSPs and agency. Internal to the agency, the federation server is integrated with an access management server and/or the applications. Integrating the federation server with the access manager enables the agency to enrich the existing authentication connection, between the access manager and the applications, with federation capabilities provided by the federation server. The integration between the federation server and access management server (or applications) is accomplished through connectors, which may require modification to the application. A connector is a small extension to a federation server, which contains the required code to perform the tasks required to establish a connection to an application. These connectors are supplied by the federation server vendor, a third party, or developed by the RP.

Figure 14 provides an overview of how the architecture requirements for an enterprise federation approach are implemented.

Architecture Requirement	Implementation Location	Number of Implementations
CSP Discovery Page	Access Management Server	Once
CSP Integration	Federation Server	Once per CSP
Assertion Parsing	Federation Server	Once
Assertion Translation	Federation Server	Once
Authorization Enforcement	Access Management Server[44]	Once
Account Provisioning and	Federation Server[45]	Once per application

[44] If the federation server directly integrates with an application, the application will have to accept the assertion for authentication.

[45] Several federation server Commercial Off-The-Shelf (COTS) products are capable of lightweight account management activities such as local profile creation and linking of users. If the agency requires more provisioning functionality, an identity manager would be needed.

Architecture Requirement	Implementation Location	Number of Implementations
Linking		

Figure 14: Solution Architecture 2 Requirements

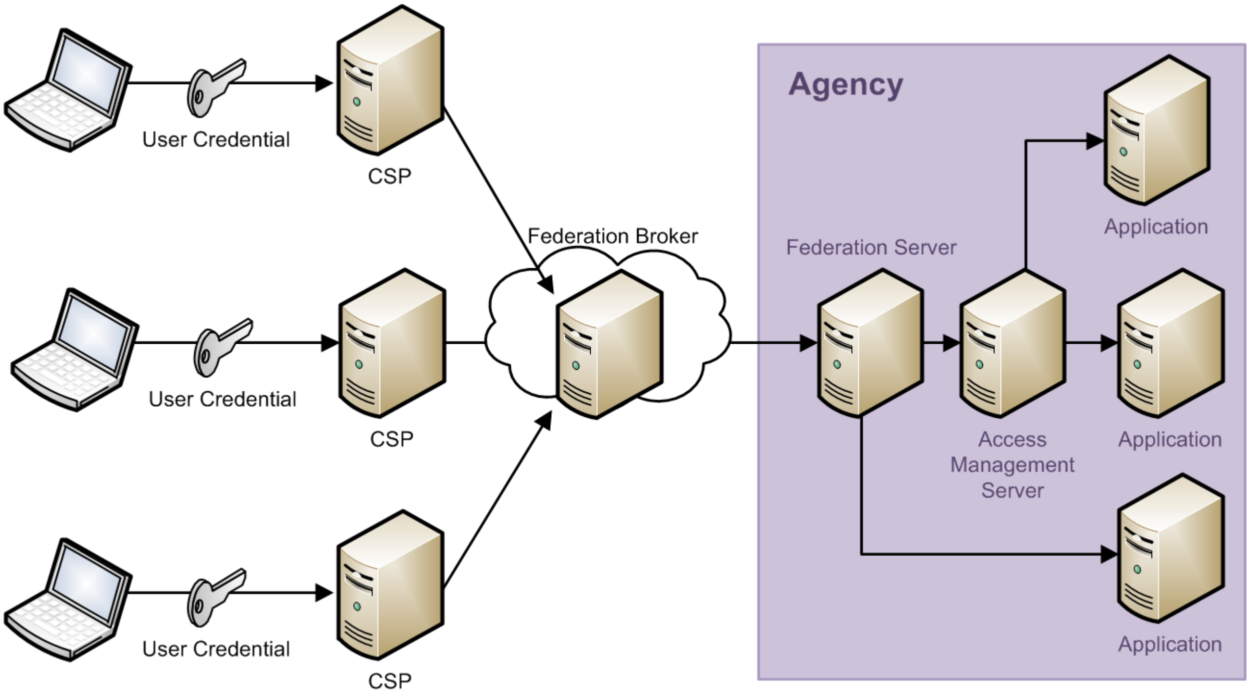
Some agencies may have already established a centralized user directory, which allows application provisioning, linking, and other similar activities to occur once at the directory, rather than once per application.

The enterprise federation architecture is a scalable and robust architecture for enabling federation within an agency. The considerations for an RP implementing this architecture include:

- Requiring more initial effort and investment than other architectural options;
- Allowing an agency to add applications and CSPs through the use of connectors, which provide a reusable framework to integrate applications with the federation server, thereby reducing future life cycle cost associated with the system.;
- Providing the ability to scale from a single application to many applications; and
- Enabling the agency to maintain control of the federation process, including selection and configuration of CSPs.

6.2.3. Federation Broker Architecture

The federation broker architecture provides infrastructure that is external to the agency that acts as a proxy between the RP and a CSP. The federation broker is a shared service model, an approach encouraged by the Federal IT Shared Services Strategy.[46] This infrastructure handles the integration with individual CSPs and the translation of the protocols that the CSP uses to one standardized format for the RP. The federation broker architecture is shown in Figure 15.



[46] Federal Information Technology Shared Services Strategy, The White House, May 2, 2012.

Figure 15: Solution Architecture 3 Federation Broker

A federation broker architecture is similar to the enterprise architecture described in Section 6.2.2; however, this architecture employs a third party (i.e., the federation broker) that creates a bridge between the CSPs and an agency. The infrastructure at the agency needs to be able to receive and parse assertions; therefore, a federation server is recommended. When establishing the secure communications channel with the federation broker, part of the configuration will include the acceptable assurance level for each RP application and the attributes that are required by the RP. Applications within the agency that are integrated with the federation server will be able to leverage the CSPs that are offered by the federation broker.

Figure 16 provides an overview of how the architecture requirements for a federation broker approach are implemented.

Architecture Requirement	Implementation Location[47]	Number of Implementations
CSP Discovery Page	Access Management Server	Once
CSP Integration	Cloud Provider	Once per CSP
Assertion Parsing	Federation Server	Once
Assertion Translation	Federation Server	Once
Authorization Enforcement	Access Management Server	Once
Account Provisioning and Linking	Federation Server	Once per application

Figure 16: Solution Architecture 3 Requirements

The federation broker provides a scalable architecture that enables the RP to outsource some of the functionality required to accept third-party credentials. The considerations for an RP implementing this architecture include:

- Removing the need for the RP to manage and configure CSP connections, including the onboarding, modification, and off-boarding;
- Providing the RP with a selection of CSPs that have been vetted by the TFPAP process, allowing the RP to choose a CSP that meets its requirements;
- Providing the ability to scale from a single application to many applications;
- Introducing security risks due to user information being passed through a third party before arriving at the RP. The RP should review the federation broker’s policies and make a determination if the trade off in security is worth the convenience of reduced integration effort;
- Limiting the selection of CSPs to those that the federation broker has available; and
- Requiring only one protocol to interact with the federation broker rather than the RP having to accommodate the protocol supported by each different CSP.

6.3. Selecting the Optimal Architectural Solution

In order for the RP to select one of the reference solution architectures discussed in Section 6.2, it is important to understand which architecture is most applicable to its situation. It is recommended that an RP leverage the information collected from the assessments during the

[47] The requirements assume the implementation of an access management server. If an access management server is not deployed, then each application will have to implement the requirements designated for the access management server.

RP's planning period to determine its optimal solution architecture. Figure 17 provides guidance to the applicability of each architectural solution. Within Figure 17, the enterprise and federation broker architecture solutions share certain situations where either one may be appropriate. These approaches both support streamlined integration of multiple applications but differ in the amount of control the agency keeps in implementing and managing the federation solution. An agency should consider each of its requirements to determine the best architectural approach.

Recommended Approach	Situations
Stand-Alone	• An agency has a small number of applications that require the acceptance of third-party credentials. • An agency wishes to pilot the acceptance of third-party credentials on a small scale before deploying it for the entire agency.
Enterprise	• An agency wishes to maintain control of which Credential Service Providers (CSPs) are integrated and the connection to those CSPs. • An agency has many applications that are required to accept third-party credentials. • An agency has existing agency-wide infrastructure that can be modified/augmented to accept third-party credentials.
Federation Broker	• An agency has many applications that are required to accept third-party credentials. • An agency has existing agency-wide infrastructure that can be modified/augmented to accept third-party credentials. • An agency wishes to accept third-party credentials from a large user base that spans many CSPs. • An agency with privacy requirements to accept externally-issued credentials without knowing to which CSP a user authenticated.

Figure 17: Guidance for Selecting an Optimal Solution Architecture

In accordance with the FICAM Roadmap, an agency should implement enterprise-level solutions/approaches where feasible to eliminate redundant investments and promote consistency and interoperability across the agency's IT infrastructure. Within the scope of this document, an agency should carefully consider the enterprise or federation broker architectures where feasible due to its alignment with the objectives of the ICAM segment architecture. As stated in the previous sections, these architectural approaches provide consistency across RP applications and lead to economies of scale, repeatable processes, simplified implementation of required security and privacy controls, and standardized troubleshooting.

7. Federation Implementation

Once an RP has selected its federation architecture, it can begin implementation of the technology solution. Two of the main elements of implementation are integrating the CSP and successful linking to an RP account. This chapter provides guidance on these elements in the following sections:

- **CSP Integration.** This section provides the RP with considerations for selecting the correct CSP, exchanging information with the CSP to achieve programmed trust, and updating the user interface to allow a user to access the application with his/her third-party credential.
- **Account Management.** This section discusses the process of creating and managing accounts for external users (i.e., non-federal users that leverage third-party credentials to gain access to federal applications). Additionally this section provides account management scenarios and examples, describes the account linking processes, and necessary maintenance activities.

7.1. CSP Integration

Integration with a CSP is critical to enabling an external user to access an RP with a third-party credential provided by the CSP. This integration enables a CSP to send an assertion to an RP, which describes a user and his/her attributes. To accomplish this, the RP should identify an acceptable CSP, determine what attributes are available from that CSP, establish a secure connection to the CSP, and modify its user interface to provide the ability for a user to authenticate with the CSP.

7.1.1. Selecting a Credential Service Provider

A key component in determining a suitable CSP is understanding the user population for a given RP application. The user population and CSP characteristics will have an impact on the CSP that is best for the RP to use. These characteristics include:

- **FICAM-approved CSPs.** An RP must select a FICAM-approved CSP. As stated in Chapter 4, the use of a FICAM-approved CSP enables trust between the RP and CSP. If it is determined that a non-approved CSP meets the requirements of the RP, then the RP can recommend the CSP work with a TFP to become FICAM-approved. The RP should not use the CSP until the CSP has been successfully approved by a TFP.
- **Availability of existing credentials.** The RP should aim to select CSPs that already serve some or all of its user population. For example, if the RP's target user population is the education community, it might seek to leverage a CSP under the InCommon federation, which is prevalent within the education community. This may increase user acceptance because it decreases the credentialing burden on the user.
- **CSP attribute availability.** If the RP requires attributes about a user, the RP can select a CSP that has the required attributes about the user. It is likely that a CSP may have only a partial set of attributes that an RP requires. In this case, the RP should determine if it can

obtain the additional attributes it needs from another source or collect additional information from the user.[48]

- **Level of assurance provided by the CSP.** The level of assurance at which a CSP has been approved should be equal to or greater than the level of assurance that the RP requires.

An RP can integrate with multiple CSPs, which enables a broader set of users to access the RP application and could increase user traffic. If the RP decides to integrate with multiple CSPs, the enterprise or federation broker architectures may be beneficial. These solution architectures enable the reuse of configurations and federal profiles for integrating with CSPs, thereby reducing the cost of integration with new CSPs.

7.1.2. Programmed Trust

Programmed trust between an RP and CSP is a mechanism to enable trusted communication between both parties. It consists of mutual authentication and the exchange of shared information (e.g., Uniform Resource Locator [URL] endpoints, allowed bindings, certificates). Mutual Authentication is the process of validating that the other party is who it claims to be and is approved to participate in the transaction in order to lessen the probability of an attack like “man in the middle” or “spoofing.” In the case of SAML, metadata provides the shared information used to achieve programmed trust. Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource.[49] During the planning period, metadata is provided to the CSP and RP about the other participant. During run-time this metadata is used to validate that the CSP or RP is indeed who they claim to be and is approved to participate in the transaction.

7.1.3. User Interface

In order to enable the acceptance of third-party credentials, an agency will need to modify the RP application login or CSP discovery page to present the user with links to acceptable CSPs. The updates to the user interface can occur at the application, federation server, or federation broker depending on the federation architecture selected in Chapter 5. When clicked, these links should redirect the user to the desired CSP with the correct parameters to assure he/she will be redirected back to the RP after authentication has taken place. The parameters that must be sent to the CSP vary depending on the protocol that is used. One common parameter is the RP’s application endpoint, which is the point to which the CSP sends the user and assertion after a successful authentication. When updating the user interface, the RP should ensure that it continues to meet user accessibility requirements.[50]

[48] The RP should only collect the attributes that it needs to process the transaction; this concept is known as minimalism in FICAM Privacy Guidance for Trust Framework Assessors and Auditors. In addition, the RP needs to gain consent from the user for any attributes it collects, including the intended use of those attributes, and the authority under which the RP is collecting the attributes.

[49] As defined in the FICAM Roadmap, Appendix B Glossary.

[50] As required by Section 508 Amendment to the Rehabilitation Act of 1973, which requires agencies to make their electronic information accessible to people with disabilities.

In accordance with the TFPAP, the CSP's user interface must be modified to capture user consent for collection of attributes about the user. Obtaining the user's consent can be accomplished by posting an adequate notice, which includes:

- A general description of the authentication event;
- The intended use of the attributes;
- The authority under which the attributes are collected; and
- A description of any disclosure or transmission of PII.

The adequate notice should be clearly displayed to the user and it should be made clear that the user is leaving the government site to authenticate at an external CSP. An adequate notice should not be a link on a page that leads to a complex privacy policy or general terms and conditions. Once user consent has been obtained, the RP can collect the requested attributes about the user. The RP should work with the CSP to identify what attributes the RP needs, per its SORN, and how it intends to use and manage the attributes. This will inform the consent notice presented to the user.

7.2. Account Management

Account management is the process of creating and managing accounts for both internal and external users. These accounts may exist within an application or, preferably, in an agency-wide identity management solution. Implementing a federation solution requires account management for external users (i.e., non-federal users that use third-party credentials), which entails the following sequential steps:[51]

- **Provisioning.** Provisioning is the process of creating an account for a user within an application or agency-wide identity management solution. This process takes place either as an out-of-band process where the creation of the user's RP account occurs before the user visits the application, or as a just-in-time process that takes place when the user first visits the application.
- **Account Linking.**[52] Account Linking is the process of associating one or more identities to an RP account based on the identifiable data passed in the assertion or from other sources. In addition, some applications may allow a user to unlink his/her federated identity from his/her local identity. Account linking is further discussed in Section 7.2.2.
- **Account Maintenance.** Account maintenance is the periodic review, modification, and/or removal of accounts in an application or agency-wide identity management solution.

During this process, a new account is created for the user, which may take place either before or during the user's initial visit to an application with a third-party credential. Provisioning is not a requirement for all applications; however, it is necessary if the application needs to maintain the state of a user across multiple visits.

After provisioning, an RP performs account linking to associate one or more identities with an RP account based on the unique identifiers passed in the assertions. Identification of the user can

[51] If provisioning is required, it must occur before all other processes in account management.

[52] Account linking, as defined in this document, is specific to the activities that occur in federated authentication and is different than the Linking/Association service defined in the FICAM Roadmap.

be accomplished up front by the CSP or once the assertion is received by the RP. In the first case, an identity can be automatically linked to a user’s RP account if the required attributes are present in the assertion. If the required attributes are not present in the assertion, a manual linking process can be performed by the RP after the assertion is received. The manual linking process allows a user to link his/her identity to the appropriate RP account by confirming his/her identity to the RP. Methods used to confirm a user’s identity are discussed in Section 7.2.2.3, Resolving Account Linking Issues. Regardless of the method used to perform account linking, the RP should only collect the minimum amount of PII necessary, consistent with the privacy-enhancing principle of data minimization.

After the user has successfully confirmed his/her identity, the RP can link the assertion to the correct RP account by storing the unique identifier contained in the assertion. This unique identifier will be used during future attempts to correlate identities with the correct RP account. Offering more than one approach allows flexibility in the account linking process.

Terminology

CSP-Performed Identity Binding – The process by which a CSP provides all required information for the RP to bind the identity within the assertion to the RP account.

RP-Performed Identity Binding – After the RP receives the assertion from the CSP, the RP collects additional information or conducts additional identity proofing in order to successfully bind the assertion to the identity.

7.2.1. Account Management Scenarios and Patterns

Account management will vary depending on the relationship between the user and the RP. This relationship will define the extent to which the RP will have predetermined information about the user. Section 12.3.1 of the FICAM Roadmap defines five provisioning scenarios that describe these relationships. Those five scenarios are:

- Business-Entity Relationship with a Known User Base;
- Business-Entity Relationship with Indeterminate User Base;
- Relationship with an Individual, Known User;
- Relationship with an Individual, Unknown User; and
- Temporary Access Session.

In the first two scenarios, where there is an existing relationship with a business entity, it is likely that the credential being leveraged for federation was issued by the business entity. Since these scenarios fall outside of accepting FICAM-approved third-party credentials, this document does not provide specific guidance on them. The remaining three scenarios involve an individual user, in this case a non-federal user, and his/her relationship with an RP. These scenarios are discussed further in the following sections.

7.2.1.1. Relationship with an Individual, Known User

This type of account management scenario requires that the user have a pre-existing relationship with the RP application and/or agency. That is, the user has interacted with the agency and the agency has a record of the user and certain attributes about the user. An example of this scenario is an agency that provides grants to a user. When the user requests a grant, he/she will provide information about himself/herself to the agency. This could result in the creation of an account at the RP application or the storage of the user’s information in a repository within the agency. In either of these cases, the agency retains the information about the user requesting a grant. Later when the user attempts to access the RP with a third-party credential, the RP can use this information to assist in account linking.

Provisioning of the RP account will occur prior to the user's initial visit to the application with his/her third-party credential. This provisioning may occur during an out-of-band process such as the creation of the record for the user when he/she requested the grant in the example above; or by having the user manually visit the application and create an RP account using local credentials (e.g., username and password). Account linking occurs when the user visits the application with his/her third-party credential. If the assertion passed to the RP does not contain the attributes required to link the user's identity from the CSP to the RP account, the RP will need to identity proof the user. Methods for accomplishing this are discussed in Section 7.2.2.3, Resolving Account Linking Issues. After the RP identity proofs the user, unique attributes from the assertion are associated with the RP account. This association, or linking, will be persistent at the RP, which allows future access attempts with the given credential to succeed without requiring the identity proofing step.

Figure 18 provides a summary of the known user account management activities.

Activity	Description
Provisioning	This activity occurs prior to the user's first attempt to access the application with a third-party credential. The Relying Party (RP) account is created, but no credential, or only a local credential, is associated with the account.
Account Linking	Upon first attempting to access the application, the user's credential is associated with his/her RP account. Additional credentials can be associated with an RP account at any time, if the application employs the *single account multiple credentials* pattern discussed in Section 7.2.2.1.
Account Maintenance	The implementation of these activities is at the discretion of the RP. Please refer to Section 7.2.3 for more information on the activities that comprise account maintenance.

Figure 18: Individual, Known User Account Management Activities

7.2.1.2. Relationship with an Individual, Unknown User

This type of account management scenario does not require the RP account to be provisioned before the user's initial visit to the application with his/her third-party credential. An example of this scenario is a user that attempts to access the application without being known by the agency. The RP application will receive an assertion from a CSP about the user. At this time, the RP will create a "shadow account", which is an RP account that is created for the purpose of maintaining a persistent association with an external user. The unique identifier within the assertion is linked to the shadow account.

Lesson Learned

Research.gov, National Science Foundation's (NSF) grants management system, successfully allows first-time visitors to use an OpenID credential (e.g. Google) to access NSF visitor services. By provisioning the user's account to the application, NSF allows the user to personalize his/her experience for future visits, including a personalized homepage, up-to-date Research.gov news, and information through Rich Site Summary (RSS) feeds and email alerts.

In this scenario, if the RP received enough information from the assertion to uniquely identify the user, the RP will create a local RP account. Since this activity happens dynamically as the assertion is received, it is referred to as just-in-time provisioning. If the RP requires additional information to uniquely identify the user, then provisioning does not occur when the assertion is received. Instead, the RP will collect this information using one of the methods described in Section 12.3.2 of the FICAM Roadmap. The RP should only collect the minimum amount of information that is required for the user to perform a transaction with the RP. The RP will perform a level of identity proofing to vet the information obtained about the user. This can be achieved by leveraging a trusted third party or by conducting identity proofing in person. Upon completion of the identity proofing, the RP will provision an RP account for the user. This is referred to as deferred provisioning, since the provisioning activities occur at a time later than when the initial assertion is received.

Account linking takes place immediately after provisioning, associating unique attributes contained in the assertion from the CSP to the RP account that was just created. Similar to the known user scenario described in Section 7.2.1.1, the association of the CSP account to the RP account is persistent; allowing future access attempts with the given credential to succeed without requiring the identity proofing step. Figure 19 provides a summary of the known user account management activities.

Activity	Description
Provisioning	This activity occurs when the user first attempts to access the application. If the assertion contains all of the required information, the Relying Party (RP) uses that information to provision the RP account. This is referred to as just-in-time provisioning. If the assertion does not contain all of the required information, the RP can gather the missing components and provision the RP account later. This is referred to as deferred provisioning.
Account Linking	Immediately after provisioning occurs during the user's first access attempt, the user's credential is associated with his/her RP account. Additional credentials can be associated with an RP account at any time if the application employs the *single account multiple credentials* pattern discussed in Section 7.2.2.1.
Account Maintenance	The implementation of these activities is at the discretion of the RP. Please refer to Section 7.2.3 for more information on the activities that comprise account maintenance.

Figure 19: Individual, Unknown User Account Management Activities

7.2.1.3. Temporary Access Session

This type of account management scenario does not require provisioning of a permanent RP account. Some applications can provide access to the user without provisioning an account. Other applications, however, may need to provision a temporary account for the user, which will be removed when the user terminates his/her session with the application. The key difference between the temporary access scenario and other scenarios is that the user's information does not persist from session to session for the user.

Activity	Description
Provisioning	Depending on the application implementation, a temporary account may or may not be created. If it is created, the account only exists for the duration of the user's session.
Account Linking	N/A
Account Maintenance	The implementation of these activities is at the discretion of the Relying Party (RP). Please refer to Section 7.2.3 for more information on the activities that comprise account maintenance.

Figure 20: Temporary Session Provisioning Activities

7.2.2. Account Linking

This section provides a more detailed discussion around account linking, including account linking patterns, methods, and issue resolution. Account linking applies to the known and unknown user scenarios described in the previous section. In those scenarios, the RP links the user’s CSP credential to the RP account. The user should be provided adequate notice that the RP is linking his/her account and the RP should provide the user with the option to opt out of linking the credential to the RP account.

Account linking relies on the presence of an RP account to bind the credential. A user may already have an RP account, may register for an RP account when attempting to link a credential, or an RP account may be created automatically when the user presents his/her externally-issued credential for linking.

Implementation Tip

A Relying Party (RP) should provide an option for a user to create a local credential, even when its application accepts third-party credentials. This provides the RP with a means of provisioning an account for a user that does not have the required third-party credential. The use of local credentials may require the RP to perform additional identity proofing for users that create such a credential.

7.2.2.1. Account Linking Patterns

As part of provisioning and account linking, an RP will link one or multiple external credentials to an internal user account. Section 12.3.3 of the FICAM Roadmap identifies several patterns that an agency could potentially use to handle such a situation. These patterns include:

- **One account per user/credential combination.** The user has the ability to create a new RP account with each credential. This is a one-to-one linking of credentials to RP accounts and leads to several credential/RP account combinations for a single user. The credential/RP account combinations are not linked in any form.
- **One account per user regardless of the number of credentials.** The user has an RP account that is linked to one or more credentials. This is a many-to-one linking of credentials to RP accounts and allows a user to have a consistent experience regardless of the credential used to access the application. The application will need to have logic in place to associate multiple credential identifiers to a single RP account.

In addition to these two patterns, the FICAM Roadmap also identifies several other patterns that are not relevant to the acceptance of third-party credentials and therefore were not included in this document. For a complete list of patterns, please see Section 12.3.3 of the FICAM Roadmap.

7.2.2.2. Performing Account Linking

Account linking is the one time process for matching incoming credentials with the correct RP account. The linking process is accomplished by storing a unique identifier from the credential with the RP account. This allows the RP to use the unique identifier presented by the credential to identify the user’s RP account. Once account linking is performed, the correlation between the CSP account and the RP account is persistent, and for each subsequent log in the RP maintains the correlation of the CSP account to the RP account. An RP can leverage the following types of unique identifiers to perform account linking:

- **Single Attribute.** This type of identifier represents a single piece of information about a user. An example of this type of identifier is an email address.
- **Attribute Combinations.** This type of identifier consists of several pieces of information about a user, that when combined will uniquely identify the user. An example of this type of identifier can be first name, last name, date of birth, and the last four digits of your social security number.[53] RPs should consider whether new privacy risks arise when attributes are combined together.
- **Pseudonyms.** This type of identifier is a name or alias that has been assigned to a user that is different than the user's real name. The pseudonym can be self-generated by the user or it can be generated by the CSP. The linking of the pseudonym to the RP account will occur in the same fashion as the single attribute.
- **Random Unique Identifier.** This type of identifier is a single attribute that is random and has no meaning. Each individual user is assigned a random identifier by the CSP that the RP associates with the user's RP account. The PPID[54] is a random unique identifier that is different for each RP/user combination. It allows a user to access various government applications without being tracked across those applications. A user's PPID will be different between RPs, however, it will be persistent for a single RP, serving as the correlation key between the CSP account and the RP account for all future authentication events.

The attributes used to link a user's account may be available from the CSP and provided in the assertion or the RP may determine the attributes from another source. For additional methods of collecting information about a user, please see Section 12.3.2 of the FICAM Roadmap.[55]

In the case of single attribute or attribute combination, the CSP provides attributes that have meaning to the RP and can be used by the RP to identify a user. When the attribute is passed through an assertion, the RP will have the corresponding information to link the CSP account to the RP account. In the case of the random unique identifier, or PPID, if the RP has predetermined knowledge of the PPID, then it can use the PPID to link the CSP account to the RP account. Typically the RP will not know the PPID ahead of time and will have to use other means to perform the initial account linking. This is shown in Figure 21.

[53] Per M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable

Information, OMB, May 22, 2007 [M-07-16], the Federal Government is reducing its reliance on Social Security Numbers.

[54] See Section 4.2 for a description of the PPID.

[55] FICAM Roadmap

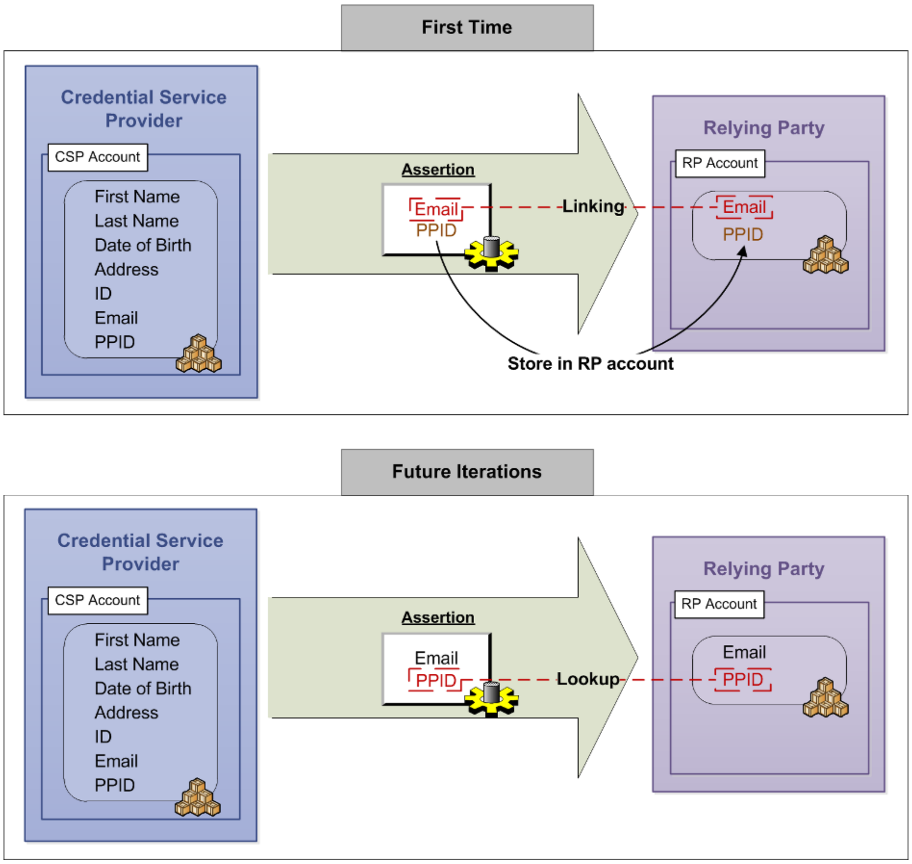


Figure 21: Account Linking using the PPID

Figure 21 illustrates using the single attribute method to perform the initial account linking and the PPID for future correlation between the CSP account and RP account. In this method, the first time the RP receives an assertion for a given user, the RP will match the email, as an example, in the assertion to the user's local RP account and link the CSP account to the RP account. At this point, the RP will store the PPID that was sent in the assertion and associate it with the RP account. In future iterations where the RP receives an assertion about the same user, it can then use the PPID to lookup the RP account. In this example, the single attribute account linking method was used for the initial account linking; however, other methods such as the multiple attribute or pseudonym can be used as well.

FAQ

What are examples of attributes that uniquely identify a person?
Common attributes used for identification include first name, last name, full address, date of birth (DOB), and Social Security Number (SSN).[56] The Relying Party (RP) can also use variations of these attributes such as the last four digits of the SSN, city, and state. Combinations of these attributes can provide a high level of confidence for uniquely identifying a user.

[56] Per M-07-16, the Federal Government is reducing its reliance on Social Security Numbers.

When choosing a unique identifier,[57] it is imperative that the value will not change over time. If the value of the unique identifier does change, the users will lose access to his/her RP account, thus forcing the user to call the help desk to resolve the problem.

Linking can either be an automated or manual process. An automated process compares unique identifiers in the assertion to unique identifiers in the RP accounts; if a match is found, the credential is automatically correlated to the account. The manual process allows the user to link credentials to an RP account through login verification or by providing a shared secret known only by the user and the RP. With login verification, the user will initially log in with his/her local RP account and then with the desired CSP credential he/she wishes to link. When the assertion from this new credential is returned, the unique identifier from the credential can be linked to the user's RP account. Alternatively, the user can link his/her account to the RP based on a known shared secret. The user logs into the application with his/her third-party credential. The application then prompts the user to enter the shared secret (e.g., unique information provided to the user in an out-of-band manner), which the user provides. The application will perform a lookup within the RP application to determine the RP account that matches the shared secret. If that match is found, the user credential used to log in is linked to the RP account. RPs should strive to provide both automated and manual linking processes. This provides a backup mechanism for linking credentials to RP accounts when the automated process does not succeed.

7.2.2.3. Resolving Account Linking Issues

If initial account linking is not successful, the RP should have additional mechanisms in place to assist the user in linking his/her account. These mechanisms should allow the RP to uniquely identify the user, thus allowing the application to link the credential to the correct identity (if the correct identity exists). Methods that an RP can use to resolve account linking issues include:

- **In-person identity verification.** This method requires the user to visit an in-person location to provide additional information about his/her identity. In-person identity verification enables an RP to gather other identity information to link the user's identity to his/her RP account.
- **Trusted third party.** This method redirects a user to a third-party site (e.g., Experian) where he/she is prompted with several questions to verify his/her identity.
- **Help desk/call center.** This method requires the user to call the help desk to resolve linking issues. The help desk can ask a series of questions to verify his/her identity.

7.2.3. Account Maintenance

Once the previous account management processes, such as provisioning, have been carried out successfully, account maintenance processes begin. Processes within account maintenance include:

- **Performing Account Cleanup.** The implementation of account cleanup is highly dependent upon how often users access the application. For many applications, it is normal to deactivate a user account after an extended period of inactivity. However, an application that users access on an infrequent basis will require an inactivity time that is

[57] For a more detailed discussion on unique identifiers, please refer to Section 7.1.3.1 of the FICAM Roadmap.

of appropriate length. One method for handling this is to send a notification to the user in advance of deactivating his/her account to allow him/her ample time to log in and reset the inactivity timer.

- **Unlinking Federated Identities.** In addition to linking credentials to an RP account, the user should also be provided a method to unlink his/her credentials from the RP account. Unlinking can be initiated by a user or by the RP. From the user's perspective, allowing unlinking provides the user with the ability to opt out of using his/her third-party credential for the RP application. From an RP perspective, it gives the RP the ability to unlink the account of a user if a given CSP is no longer trusted. The RP needs to determine if the user can unlink all third-party credentials from his/her RP account or if at least one credential must remain linked to the account at all times. If all credentials can be removed from the account, the RP may want to consider providing the user with a local credential to allow him/her to retain access to the application.
- **Updating RP Account Attributes.** Upon creation of the RP account, attributes about the user are stored with the RP account. These attributes may become outdated if the user does not access the application for a period of time; therefore, a mechanism should be in place to update these attributes on a periodic basis. The attributes that are stored and updated should only be the attributes that the RP has identified in its PIA and are required to process the transaction with the user. Mechanisms to update attributes at the RP can be found in Figure 22.

Mechanism	Description
Assertion	This method can be leveraged for attributes that are received through an assertion and allows a Relying Party (RP) to update attributes each time a user visits the application.
Manually	This method allows the user to update his/her attributes using some type of self-service process. Depending on how these attributes are processed by the RP, the RP may need to conduct additional identity proofing to verify the information.
Out-of-Band Communication	This method uses an out-of-band communication to retrieve attribute updates for a specific user. When using this method there must be an attribute source that accepts an out-of-band attribute request (e.g., utilizing the Backend Attribute Exchange [BAE]). This process can be initiated from either the RP or Credential Service Provider (CSP).

Figure 22: Account Update Mechanisms

This page is intentionally left blank

Appendix A Scenarios

The scenarios in this appendix expand upon the federation overview in Chapter 3 by providing a deeper view into the activities central to allowing users to access an RP application using third-party credentials. These scenarios follow the “Relationship with an Individual, Unknown User” and “One account per user regardless of the number of credentials” patterns described in Section 7.2. Each scenario describes the sequence of actions that take place, the entities involved, and data that is exchanged. Each scenario includes the following:

- **Scenario Overview.** Overview of the assumptions, preconditions, actors, triggers, and post conditions for the specific scenario.
- **Process Diagram.** Graphical overview of the steps in each scenario.
- **Process Flow.** Description of each step involved in executing the scenario. In this section, there is a table for the main process flow and possibly several alternate process flow tables. Each step in the main flow is denoted with “M” proceeded by the step number, and each step in an alternate flow is denoted with “A” proceeded by the step number. The flow of events starts at the top of the table and flows to the bottom unless an alternate flow is noted in the “Alternate Flow Mapping” column. In such a case, the flow of events either continues to the bottom of the table, ignoring the alternate flow, or proceeds to the alternate flow table.

The scenarios in this appendix are divided into two logical groups. The first group, scenarios 1-3, describes the process of a user accessing an RP for the first time, subsequent times with the same credential, and subsequent times with a different credential. The second group, scenarios 4-5, describes processes that take place after the user has been authenticated by a CSP and redirected to the RP.

There are several general assumptions made about the scenarios in this appendix to limit the number of scenarios and to avoid extraneous details. The assumptions made are as follows:

- The user initiates the chain of events by accessing the RP first, not the CSP;
- Access to the RP must be authenticated;
- The RP’s applications are web-based;
- If the user attempts to log in multiple times incorrectly he/she will be locked out (CSP dependent); and
- A scenario can be terminated at any point if the user closes his/her browser session.

Scenario 1: First Time Log in

In this scenario, a user is attempting to access an RP application for the first time, through navigating to the RP website. Upon landing on the RP page, the User will choose to authenticate using a FICAM-approved credential. The CSP will authenticate the User and send an assertion to the RP. The RP will then use this assertion to create an RP account for the User and allow the user to access the RP application. Figure 23 provides an overview of the first-time log in scenario.

Overview Topic	Scenario Overview
Assumptions	• A credential at the designated level of assurance or higher will be used to access an application. • The Relying Party (RP) will only present a list of acceptable credential types that are at a level of assurance that is equal to or higher than that of the application. For example, if the application requires Level of Assurance (LOA) 2 or higher, the login page will not display a LOA 1 credential as an option. • The RP is responsible for collecting the additional attributes for the User. • The RP will offer a local authentication mechanism.
Preconditions	• The User's information is not present within the application. • The User possesses a credential. • There is an established trust relationship between the RP and Credential Service Provider (CSP).
Actors	• User • RP • CSP
Trigger	User needs to access the application.
Post Conditions	User has access to the application.

Figure 23: Scenario 1 Overview

Process Diagram

Figure 24 illustrates the overall process flow for Scenario 1.

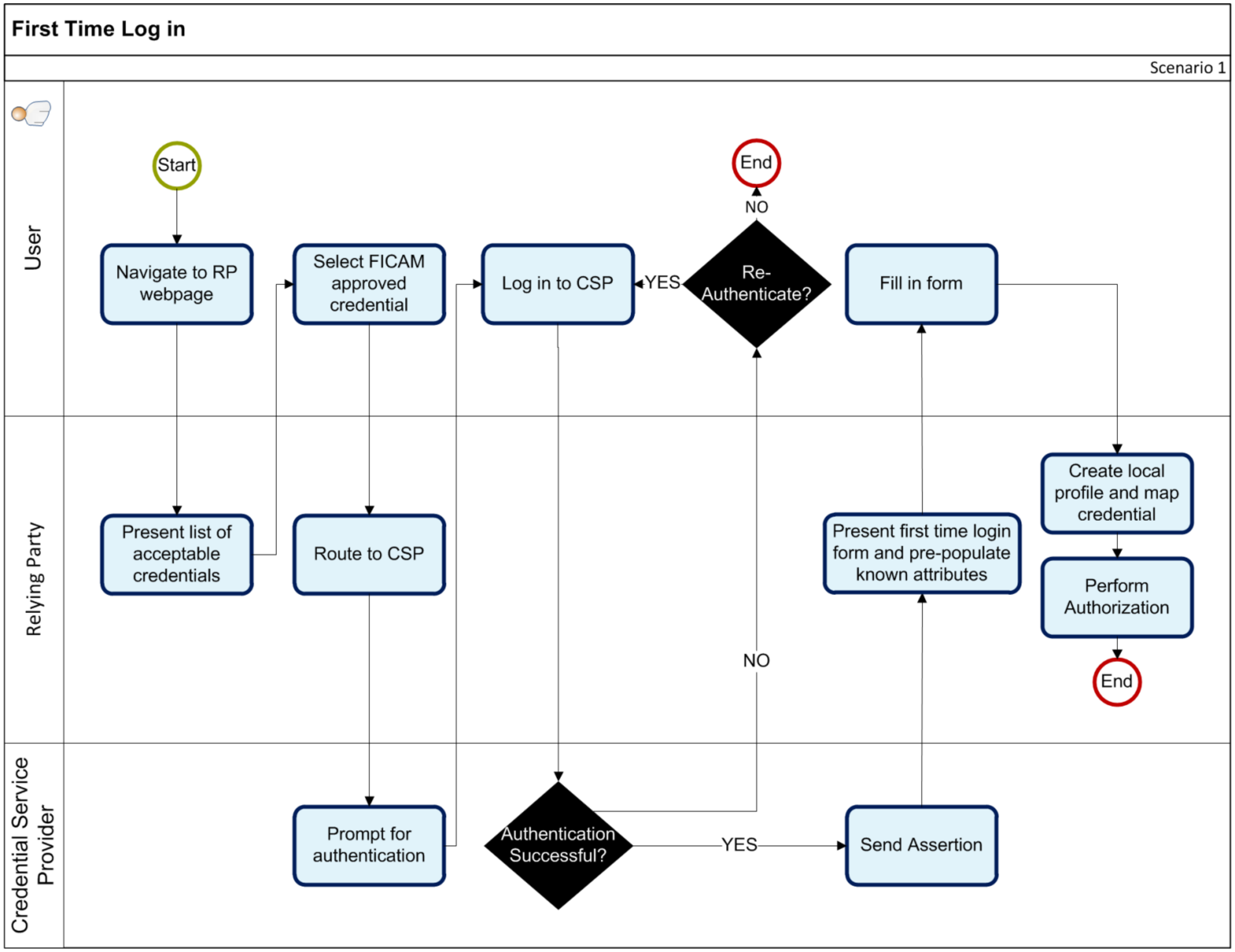

First Time Log in
Scenario 1
User
Relying Party
Credential Service Provider
Start
Navigate to RP webpage
Present list of acceptable credentials
Select FICAM approved credential
Route to CSP
Prompt for authentication
Log in to CSP
Authentication Successful?
YES
NO
Send Assertion
Re-Authenticate?
YES
NO
End
Present first time login form and pre-populate known attributes
Fill in form
Create local profile and map credential
Perform Authorization
End

Figure 24: Scenario 1 Process Diagram

Process Flow

Figure 25 provides the main process flow for Scenario 1. It describes a user attempting to access an application for the first time. During this flow, the RP allows the User to authenticate to a CSP. Failed authentication is not shown in the table below; however, it does appear in the process diagram in Figure 24. When applicable, the column on the right shows an Alternate Flow.

Step	Main Flow: Step Description	Alternate Flow Mapping
M1	User navigates to the application's publicly available login page.	
M2	Relying Party (RP) presents a list of acceptable credentials.	
M3	User selects to log in with his/her third-party credential.	
M4	Relying Party (RP) routes the User to the Credential Service Provider's (CSP) login page.	
M5	CSP requests the User to log in.	
M6	User logs into the CSP.	
M7	CSP sends an assertion including attributes to RP. *Note: If the User incorrectly enters the authentication challenge, the CSP will display an authentication fail notification. At this point the User can choose to re-authenticate, or to exit the authentication and return to the RP site.*	
M8	RP determines that the User does not have an account within the RP application.	
M9	RP presents the User with a first time registration form. *Note: This is not a required step. If the RP gets the required attributes that it needs from the CSP assertion then it may choose to skip straight to step M12. However, if this is done the RP needs a mechanism to determine that the account is unique.*	
M10	RP populates the first time registration with attributes from the credential.	
M11	User fills in the remainder of the attributes on the first time registration form.	
M12	RP provisions an account for the User.	
M13	RP links the credential used to log in to the User's newly provisioned RP account.	
M14	RP performs authorization and grants User access to RP application.	
M15	Scenario ends.	

Figure 25: Scenario 1 Main Flow: First Time Log in

Scenario 2: Subsequent Log in with a Previously Provisioned Credential

In this scenario, a user attempts subsequent access to an RP, as the User has accessed the RP site before using a third-party credential. The User returns to the RP site and will authenticate using the same FICAM-approved credential as before. Once the CSP sends the assertion to the RP, the RP will recognize that the User has previously authenticated using this credential and will identify the User's RP account within the application. Figure 26 provides an overview of the subsequent log in with a previously provisioned credential scenario.

Overview Topic	Scenario Overview
Assumptions	• A credential at the designated level of assurance or higher will be used to access an application. • The Relying Party (RP) will only present credentials that are at a level of assurance that is equal to or higher than that of the application. For example, if the application requires Level of Assurance (LOA) 2 or higher, the login page will not display a LOA 1 credential as an option. • The RP is responsible for collecting the additional attributes for the User. • The RP will offer a local authentication mechanism.
Preconditions	• The User is logging in to the application with the credential that has already been registered with the RP. • The User's information is present within the application. • The User possesses a credential. • There is an established trust relationship between the RP and Credential Service Provider (CSP).
Actors	• User • RP • CSP
Trigger	User needs to access the application.
Post Conditions	User has access to the application.

Figure 26: Scenario 2 Overview

Process Diagram

Figure 27 illustrates the overall process flow for Scenario 2.

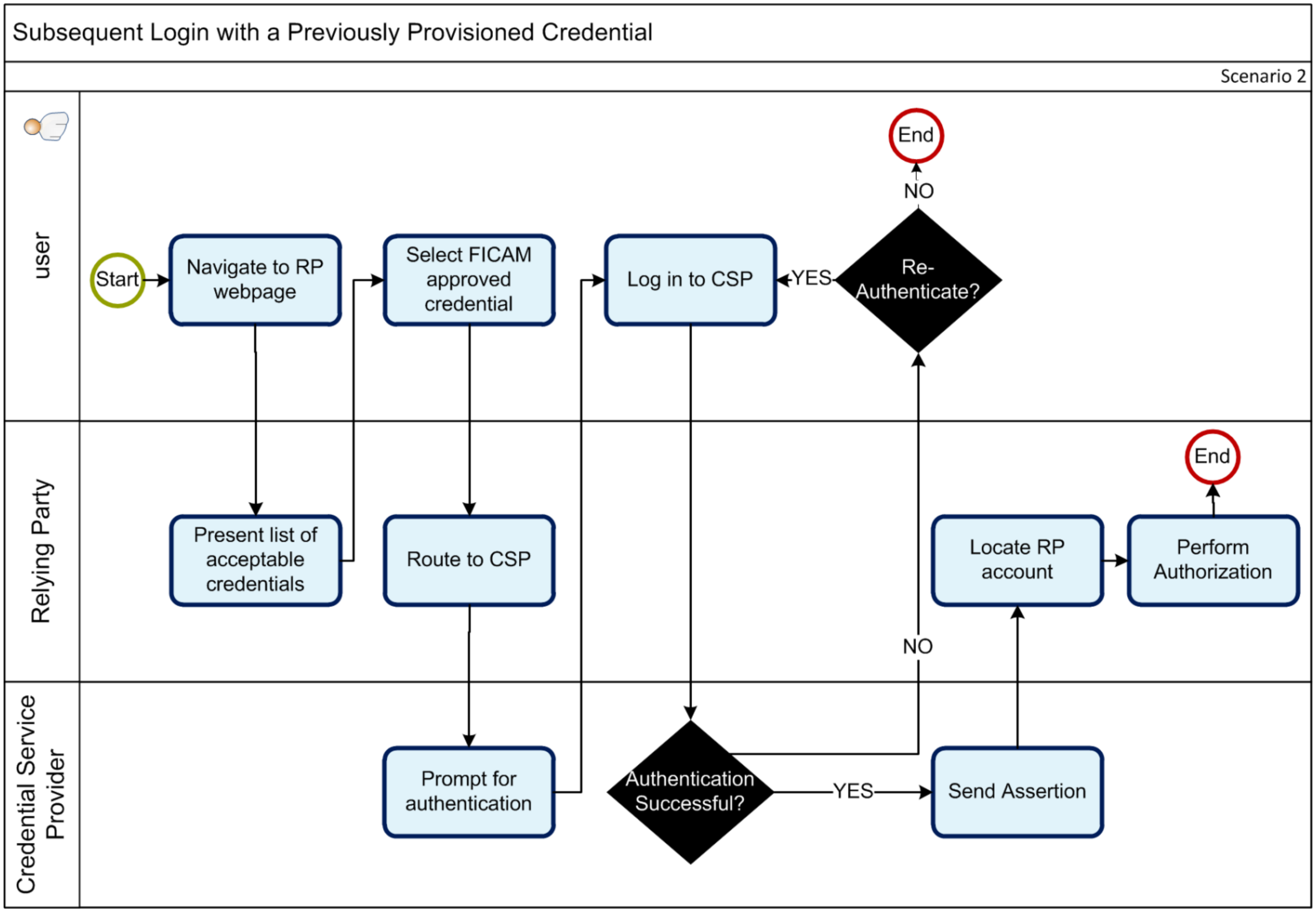

Subsequent Login with a Previously Provisioned Credential
Scenario 2
user
Relying Party
Credential Service Provider
Start
Navigate to RP webpage
Select FICAM approved credential
Log in to CSP
YES
Re-Authenticate?
NO
End
Present list of acceptable credentials
Route to CSP
Locate RP account
Perform Authorization
End
NO
Prompt for authentication
Authentication Successful?
YES
Send Assertion

Figure 27: Scenario 2 Process Flow Diagram

Process Flow

Figure 28 provides the main process flow for Scenario 2. It describes subsequent log in attempts by a user. During this flow, the RP allows the User to authenticate to a CSP. Failed authentication is not shown in the table below; however, it does appear in the process diagram in Figure 27. When applicable, the column on the right shows an Alternate Flow.

Step	Main Flow: Step Description	Alternate Flow Mapping
M1	User navigates to the application's publicly available login page.	
M2	Relying Party presents a list of acceptable credentials.	
M3	User selects to log in with his/her third-party credential.	
M4	Relying Party (RP) routes the User to the Credential Service Provider's (CSP) login page.	
M5	CSP requests the User to log in.	
M6	User logs into the CSP.	
M7	CSP sends an assertion including attributes to the RP. *Note: If the User incorrectly enters the authentication challenge, the CSP will display an authentication fail notification. At this point the User can choose to re-authenticate, or to exit the authentication and return to the RP site.*	
M8	RP locates the appropriate RP account based on the assertion.	
M9	RP performs authorization and grants User access to RP application.	
M10	Scenario ends.	

Figure 28: Scenario 2 Main Flow: Subsequent Log in with a Previously Provisioned Credential

Scenario 3: Subsequent Log in with a Different Credential

In this scenario, a User attempts subsequent access to an RP. The User had previously accessed the RP site using a FICAM-approved credential; however, when the User returns to the RP site he/she leverages a different FICAM-approved credential to authenticate. The RP will not have seen this credential before and will need to identify that the User's RP account already exists. When this occurs, it is important that the RP be capable of correlating the accounts together. This scenario assumes that the RP requires one unique account per user regardless of the number of credentials[58] and that all externally-issued credentials for that user must be linked to his/her one account. Figure 29 provides an overview of the subsequent log in with a different credential scenario.

Overview Topic	Scenario Overview
Assumptions	• A credential at the designated level of assurance or higher will be used to access an application. • The Relying Party (RP) will only present credentials that are at a level of assurance that is equal to or higher than that of the application. For example, if the application requires Level of Assurance (LOA) 2 or higher, the login page will not display a LOA 1 credential as an option. • The RP is responsible for collecting the additional attributes for the User. • The RP will always offer a local authentication mechanism.
Preconditions	• The User's information is present within the application. • The User possesses a credential. • There is an established trust relationship between the RP and Credential Service Provider (CSP).
Actors	• User • RP • CSP
Trigger	User needs to access the application.
Post Conditions	User has access to the application with a different credential.

Figure 29: Scenario 3 Overview

[58] See Section 7.2.2.1 for a description of the one unique account per user regardless the number of credentials scenario.

Process Diagram

Figure 30 illustrates the overall process flow for Scenario 3.

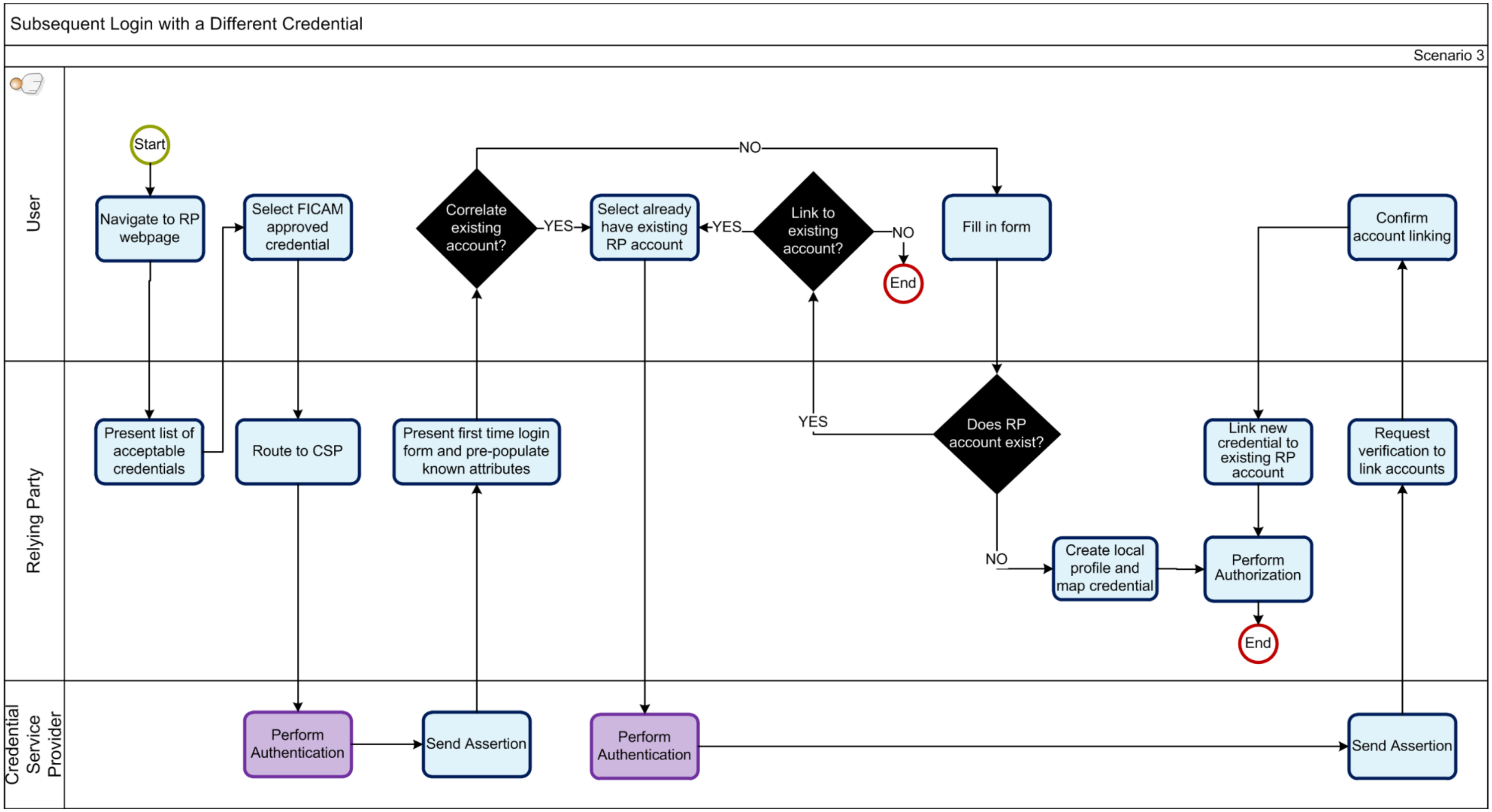

Subsequent Login with a Different Credential
Scenario 3
User
Relying Party
Credential Service Provider
Start
Navigate to RP webpage
Select FICAM approved credential
Correlate existing account?
YES
NO
Select already have existing RP account
YES
Link to existing account?
NO
End
Fill in form
Confirm account linking
Present list of acceptable credentials
Route to CSP
Present first time login form and pre-populate known attributes
YES
Does RP account exist?
NO
Link new credential to existing RP account
Request verification to link accounts
Create local profile and map credential
Perform Authorization
End
Perform Authentication
Send Assertion
Perform Authentication
Send Assertion

Figure 30: Scenario 3 Process Flow Diagram

Process Flow

Figure 31 provides the main process flow for Scenario 3. It describes subsequent log in attempts by a user. In this flow, the User will choose to log in with a new credential and associate it with an RP account that already exists in the application. Failed authentication is not shown in the table below; however, it does appear in the process diagram in Figure 30. When applicable, the column on the right shows an Alternate Flow.

Step	Main Flow: Step Description	Alternate Flow Mapping
M1	User navigates to the application's publicly available login page.	
M2	Relying Party (RP) presents a list of acceptable credentials.	
M3	User selects to log in with his/her third-party credential.	
M4	Relying Party (RP) routes the User to the Credential Service Provider's (CSP) login page.	
M5	CSP requests the User to log in.	
M6	User logs into the CSP.	
M7	CSP sends assertion including attributes to the RP. *Note: If the User incorrectly enters the authentication challenge, the CSP will display an authentication fail notification. At this point the User can choose to re-authenticate, or to exit the authentication and return to the RP site.*	
M8	RP presents the User with a first time registration form. *Note: This is not a required step. If the RP can identify that the account already exists based on a set of attributes, then the RP can prompt the User to correlate the accounts. In this case, go to step M11.*	
M9	User selects the option in the form for having an existing RP account.	Alternate Flow 1
M10	Repeat steps M2 through M7.	
M11	RP identifies the existing RP account in the database and requests the User to verify the existing account. *Note: This verification can be done via email, out-of-band communication, challenge/response, etc.*	
M12	User confirms the account correlation.	
M13	RP correlates the new credential to the existing RP account. *Note: In this context, a new credential refers to the credential that has not already been correlated to an RP account.*	
M14	RP performs authorization and grants User access to RP application.	
M15	Scenario ends.	

Figure 31: Scenario 3 Main Flow: Subsequent Log in with a Different Credential

Figure 32 provides the alternate process flow for Scenario 3. In this alternate flow, the User does not choose to correlate his/her new account with his/her existing account. However, based on the attributes in the assertion and the information collected from the User, the RP determines that the attributes match another existing account.

Step	Alternate Flow 1: Step Description	Alternate Flow Mapping
A1	Relying Party (RP) presents the User with a first time registration form.	
A2	RP populates the first time registration with attributes from the credential.	
A3	User fills in the remainder of the attributes on the first time registration form.	
A4	RP determines that the User's RP account already exists based on the attributes collected.	
A5	User chooses to link CSP account to his/her existing RP account. *Note: If the RP determines that an RP account with the supplied attributes already exists and the user does not want to link the CSP account to the RP account, then the user cannot access the RP with the new account and the scenario ends.*	
A6	Go to main flow step M11.	M11

Figure 32: Scenario 3 Alternate Flow 1: Automatic Correlation

Scenario 4: Assurance Level Escalation

In this scenario, the RP requires a user to re-authenticate using a higher level of assurance credential than used during his/her initial log in. During the initial risk assessment for the application it has been determined that the application has features that can be accessed at varying levels of assurance. The User authenticates to the RP application initially using the lowest level of assurance credential acceptable by the RP application. Subsequently, the User attempts to access a feature of the application that requires a higher level of assurance. At this point, the RP will prompt the User for re-authentication. Figure 33 provides an overview of the assurance level escalation scenario.[59]

Overview Topic	Scenario Overview
Assumptions	• A credential at the designated level of assurance or higher will be used to access an application. • The Relying Party (RP) is capable of validating policies. • The User has previously logged in with the credential being used and it has been correlated to his/her account.
Preconditions	• The User possesses a credential at the correct level of assurance for the desired function. • There is an established trust relationship between the RP and Credential Service Provider (CSP). • User is already authenticated and in the application.
Actors	• User • RP • CSP
Trigger	User needs to use a feature of the application that requires a higher level of assurance than the credential that he/she logged in with provides.
Post Conditions	User has access to the feature of the application.

Figure 33: Scenario 4 Overview

[59] Additional guidance on assurance level escalation can be found in Section 6.5.1 of SP 800-63.

Process Diagram

Figure 34 illustrates the overall process flow for Scenario 4.

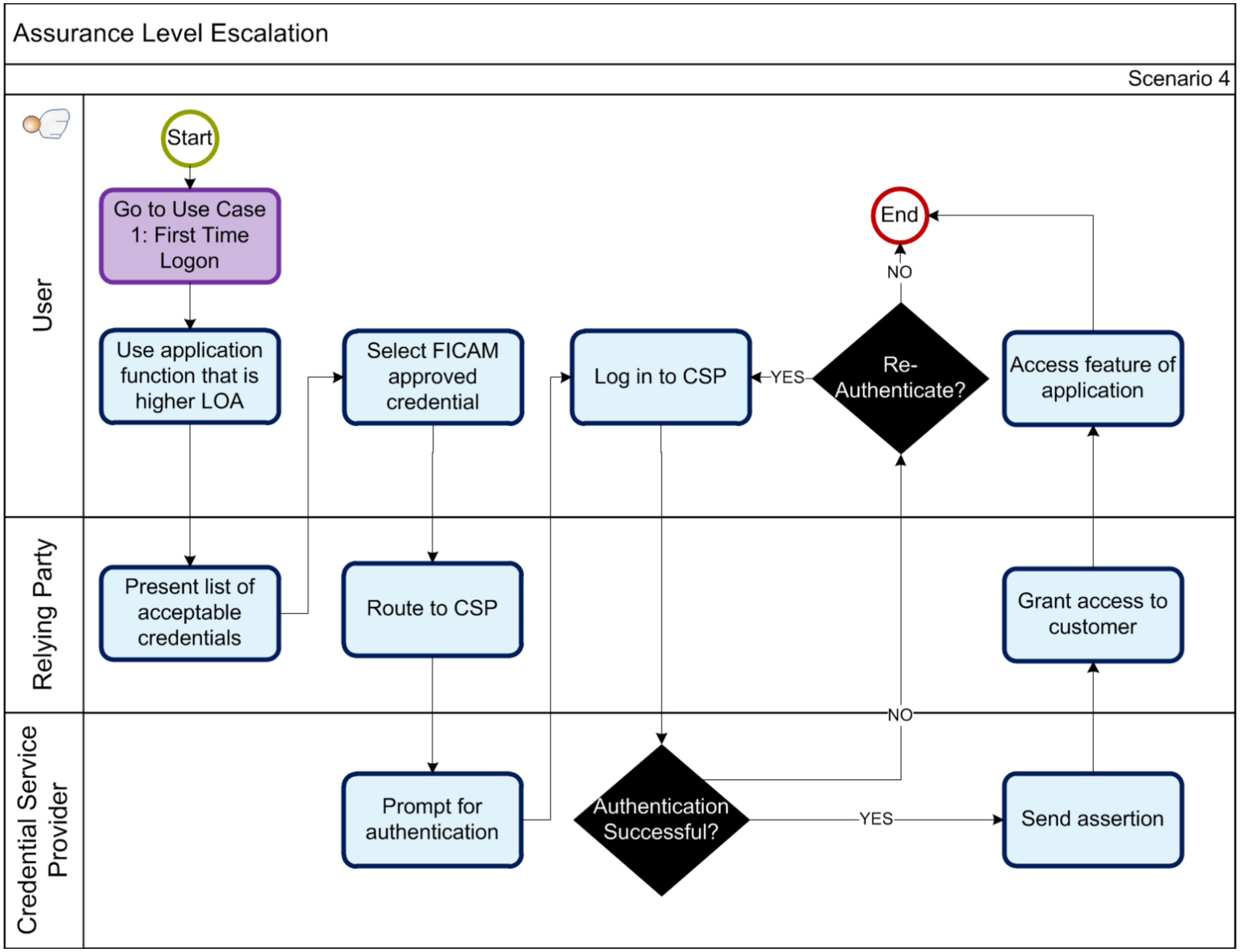

Assurance Level Escalation
Scenario 4
User
Relying Party
Credential Service Provider
Start
Go to Use Case 1: First Time Logon
Use application function that is higher LOA
Present list of acceptable credentials
Select FICAM approved credential
Route to CSP
Prompt for authentication
Log in to CSP
Authentication Successful?
YES
NO
Send assertion
Grant access to customer
Access feature of application
Re-Authenticate?
YES
NO
End

Figure 34: Scenario 4 Process Flow Diagram

Process Flow

Figure 35 provides the main process flow for Scenario 4. It describes the flow for a user to re-authenticate with a higher level of assurance credential. Failed authentication is not shown in the table below; however, it does appear in the process diagram in Figure 34. When applicable, the column on the right shows an Alternate Flow.

Step	Main Flow: Step Description	Alternate Flow Mapping
M1	User attempts to access a function of the application that requires a higher level of assurance than provided by the initial credential.	
M2	Relying Party (RP) asks the User to re-authenticate.	
M3	RP presents a list of acceptable credentials.	
M4	User selects to log in with his/her third-party credential.	
M5	RP routes the User to Credential Service Provider's (CSP) login page.	
M6	CSP requests the User to log in.	
M7	User logs into the CSP. *Note: If the User incorrectly enters the authentication challenge, the CSP will display an authentication failure notification. At this point the User can choose to re-authenticate, or to exit the authentication and return to the RP site.*	
M8	CSP sends an assertion including attributes to the RP. *Note: The RP may choose to ask the user to link the CSP account at the higher assurance level to the RP account for the user. In this way, the RP can maintain a link to additional RP accounts, making future authentications with those accounts easier for the user.*	
M9	User accesses the function of RP.	

Figure 35: Scenario 4 Main Flow: Assurance Level Escalation Authentication

Scenario 5: Retrieve Additional Attributes

In this scenario, the RP has determined that additional attributes are needed about a user in addition to what it received in the assertion from the CSP. These attributes could be for authentication, authorization, or a variety of other purposes. The RP will identify the Attribute Provider for the given attribute and communicate with the Attribute Provider to retrieve the required attributes. Figure 36 provides an overview for the retrieve additional attributes scenario.

Overview Topic	Scenario Overview
Assumptions	• An Attribute Provider exists with the desired attribute about the User. • The Relying Party (RP) has a mechanism to find the Attribute Provider and obtain the necessary attributes.
Preconditions	• An attribute contract exists between the Attribute Provider and the RP for the given set of attributes. • There is an established trust relationship between the RP and Attribute Provider. • RP has received an authentication assertion from the Credential Service Provider (CSP).
Actors	• RP • Attribute Provider
Trigger	The RP requires additional attributes about a User.
Post Conditions	RP receives required attributes from the Attribute Provider.

Figure 36: Scenario 5 Overview

Process Diagram

Figure 37 illustrates the overall process flow for Scenario 5.

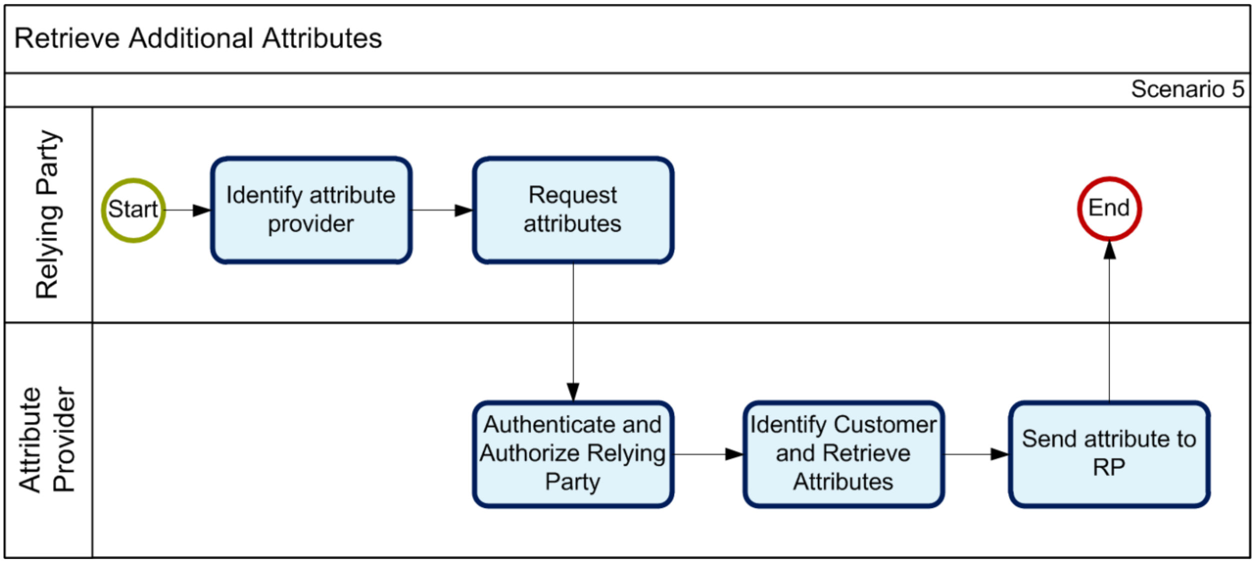

Retrieve Additional Attributes
Scenario 5
Relying Party
Attribute Provider
Start
Identify attribute provider
Request attributes
End
Authenticate and Authorize Relying Party
Identify Customer and Retrieve Attributes
Send attribute to RP

Figure 37: Scenario 5 Process Flow Diagram

Process Flow

Figure 38 provides the main process flow for Scenario 5. The main flow describes the flow of events for a successful exchange of attributes between the RP and Attribute Provider. When applicable, the column on the right shows an Alternate Flow.

Step	Main Flow: Step Description	Alternate Flow Mapping
M1	Relying Party (RP) identifies the Attribute Provider with the required attributes.	
M2	RP requests the attributes from the Attribute Provider.	
M3	Attribute Provider authenticates and authorizes the RP.	
M4	Attribute Provider identifies the User and retrieves the desired attributes.	
M5	Attribute Provider sends the attributes to the RP.	
M6	Scenario ends.	

Figure 38: Scenario 5 Main Flow: Retrieve Additional Attributes

Appendix B Case Study: National Institutes of Health

The Challenge

The U.S. Department of Health and Human Services' National Institutes of Health (NIH) conducts and supports biomedical research. NIH has a large population of external users as they provide financial support to researchers around the world and invests over $28 billion in medical research per year. NIH needed a way to grant access to these users to a variety of NIH applications.

The Solution

In order to create a more collaborative environment for NIH, NIH iTrust was implemented which is a multifunction SSO and federated authentication service consisting of:

- **NIH Login.** Links internal users at NIH to internal and departmental Health and Human Services (HHS) applications and electronic resources. NIH Login has been in production since 2003 and has over 55,000 NIH users, 275 applications, and 700 URLs resulting in 1.7 to 2.4 million transactions per day.
- **NIH Federated Login.** Links external users to NIH and departmental (HHS) applications and resources. NIH Federated Login has been in production since 2008.

In order to assist in these federation efforts, in particular NIH Federated Login, NIH leveraged federated authentication partners.

- **InCommon Federation.** Identity and access management federation for higher education and research communities. Nearly 50 major universities access NIH resources through InCommon.
- **Open Identity Exchange (OIX), OpenID, and Information Card Foundations.** NIH worked with industry leaders such as AOL, Equifax, Google, PayPal, VeriSign, and Yahoo to provide access at levels of assurance 1 through 4.

The Result

Today, NIH has increased university participation by 240%, from less than 20 university partners to approximately 60 federated university partners, with over 120,000 external credentials (an average of 2,000 to 3,000 users per week) as a result of NIH Federated Login. In particular, two specific applications have seen tremendous growth:

- **PubMed2.** Since the initial launch to leverage externally-issued credentials across its websites, the number of users leveraging externally-issued credentials to access NIH sites has grown to more than 72,000. NIH estimates that its identity management initiative will result in cost avoidance of more than $2.98 million for fiscal years 2011 through 2015. These savings will result from not having to manage user IDs and passwords for external users across approximately 50 systems.
- **iTrust.** By accepting trusted third-party credentials, the NIH iTrust program has been able to eliminate the need to issue and manage separate credentials for over approximately 100,000 non-federal users and provide these users with streamlined access to approximately 100 federated applications.

As discussed in the previous example, leveraging externally-issued credentials can enhance user traffic to agency applications through a secure means of access while realizing cost savings.

Appendix C Case Study: Homeland Security Information Network

The Challenge

Effective information sharing is critically dependent on efficient interoperability and requires robust security approaches that ensure the safeguarding and validity of data passed between systems. The Secretary of the Department of Homeland Security (DHS), Janet Napolitano, stated that "Information sharing between DHS and State governments is particularly critical to our security. Information sharing is also what makes response efforts effective. The creation of a seamless network we can use to share this information among these levels of government is a critical part of improving our partnerships."[60] In an effort to increase collaboration and information sharing, several operational challenges were identified. These include:

- The proliferation of Communities of Interests (COI) operating in silos that had pertinent information;
- The lack of a trust mechanism to ensure the security and validity of the information provided by the COIs;
- The countless number of DHS portals necessary for access to COIs;
- The multiple DHS partner components targeting the same user base; and
- The increase of COIs to address separation of information sharing and established silos of content.

The Solution

To solve this challenge, DHS implemented the Homeland Security Information Network (HSIN), a web-based, unclassified information sharing platform supporting federal and non-federal partners to establish awareness, collaborate and share information. In attempting to connect the various COIs, the first two releases of HSIN identified the following needs:

- SSO across the entire HSIN program;
- SSO federated across multiple HSIN and DHS organizations;
- Strong network of Trusted Identities across a large and diverse set of Stakeholders;
- Secure and protect user identities, system access, and information resources;
- Efficient access control for information resources;
- Fast response time to changing relationships; and
- Adopt a complete, integrated, modular approach to manage users and control resource access.

HSIN provides DHS the mechanism necessary to fight against terrorism, secure nations, enforce immigration laws, and respond to natural disasters. Over the past five years, HSIN has grown from a system deployed in two states and the District of Columbia to a system deployed in all 50 states, with more than 40 fusion centers, 53 major urban areas, five U.S. territories and several international partners. The current release of HSIN, HSIN Release 3 (R3), is an information

[60] Testimony of Secretary Janet Napolitano before the House Committee on Homeland Security on DHS, The Path Forward, DHS, February 25th 2009.

sharing model that put the network in the position to evolve from a “need to know” to “responsibility to provide” environment. R3 replaces the first two iterations of HSIN, HSIN Legacy and HSIN NextGen respectively.

R3 provides the program with a more comprehensive identity and access management solution to uniquely identify a user, manage his/her credentials, eliminate redundant identities, reuse credentials, and establish a foundation of trust and interoperability within the HSIN program and external partners. The HSIN solution components can be seen in Figure 39.

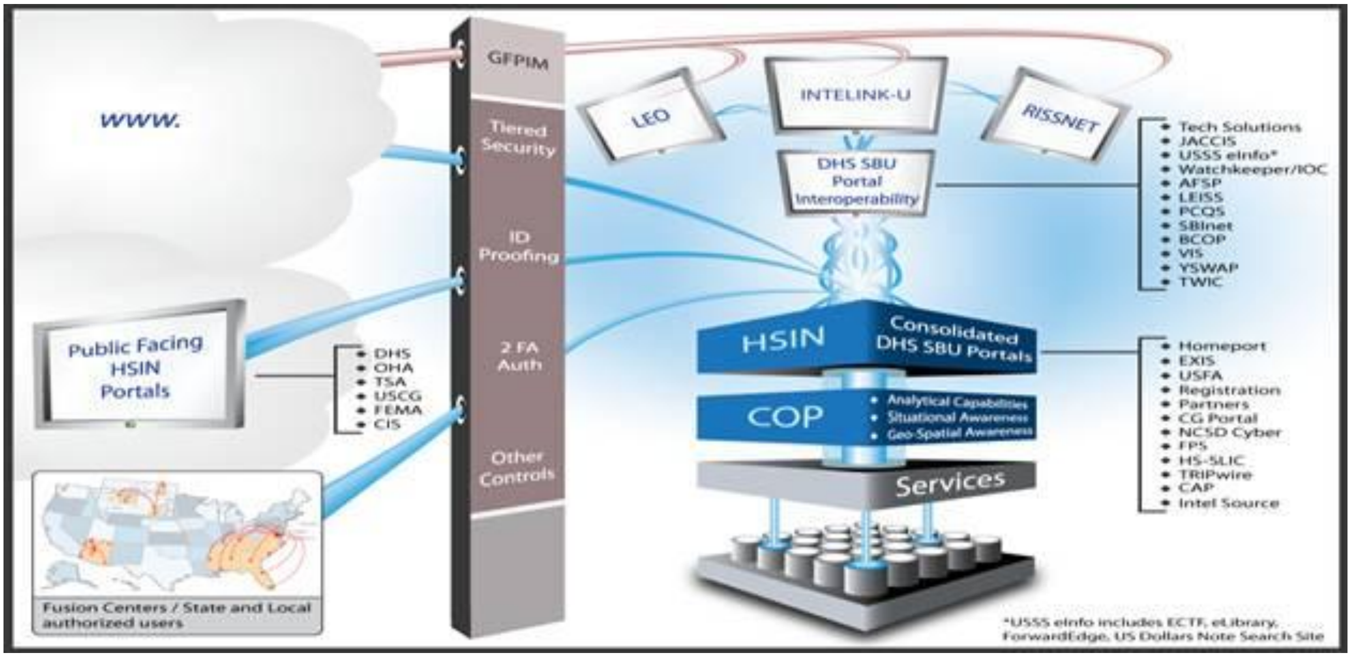


Figure 39: HSIN Solution

HSIN R3 leverages an Enterprise-Grade Identity and Access Management solution that provides Federated information sharing between partners engaged in the Homeland Security mission. R3 follows the governance model set by National Information Exchange Federation (NIEF), which leverages the Global Federated Identity and Privilege Management (GFIPM) framework and work products to provide a standards-based approach for implementing federated identity. The focus areas of R3 include:

Focus Area	Description
Account Management	• Registration, enrollment, provisioning • Support multiple directory stores for authoritative sources • Support for Active Directory/Open LDAP
Identity Proofing	• Support for persona (knowledge based) and financial (Equifax integrated) record validation • Re-identity proof based pre-determined frequency
Credential Store	• Ability to store users in a secure database and support integration with external systems through LDAP • Flexible attribute exchange model • Entitlements management

Focus Area	Description
Strong Authentication	• Single sign-on (SSO) with DHS accounts • Soft tokens (multi-factor authentication support)- One Time Password (OTP) via SMS, phone, and email • PIV and PIV-I card support
Entitlements	• Coarse grain vs. fine grain access • XACML: Policy Enforcement Point (PEP), Policy Decision Point (PDP), and Policy Access Point (PAP) • Dynamic Claims Augmentation
Federation	• Support for multiple PEPs • Support WS* and SAML protocols • Support for Active Directory; Active Directory Federation Services • Support for OIF

Figure 40: R3 Focus Areas

The Result

HSIN R3 has positioned HSIN and DHS to work towards the goal of more effectively sharing information among federal, local, tribal, territorial, state, international, and private sector organizations. R3 enables HSIN to execute its vision and mission of borderless information sharing and knowledge management within the Homeland Security Communities of Practice, and to provide stakeholders across the Homeland Security Enterprise with effective and efficient collaboration for decision making, tiered secure access to data, and accurate, timely information sharing and situational awareness. HSIN R3 provides the following benefits:

- Cross community sharing;
- Intelligence in information sharing (Fusion Center);
- Integrated and efficient approach to identity management;
- Usability integration through identity governance and the ability to federate;
- Increased security to support authentication at various security levels;
- Standards including OAuth, OpenID, XACML, and SAML; and
- Enterprise services for ICAM.

This page is intentionally left blank

Appendix D Application Questionnaire Example

This questionnaire includes sample questions for conducting an application assessment prior to integration with a federation solution, as discussed in Section 5.2.

Application Specific ICAM Questions

General

#	Questions	Answer
1	What is the full name of the application?	
2	What is the full version?	
3	Who administers the application? Need name/phone/email/address.	

Figure 41: General Questions

Application Support

#	Questions	Answer
1	Who supports the application? Need name/phone/email/address.	
2	What operating systems does this application support?	
3	What is the maintenance window, service window or service level agreement (SLA) for the application?	
4	What is the current support volume for this application (number of tickets per day)?	

Figure 42: Application Support Questions

Business

#	Questions	Answer
1	What is the business purpose of the application?	
2	Who is the business sponsor for the application? Need name/phone/email/address.	
3	Who is the technical sponsor for the application? Need name/phone/email/address.	
4	Who are the primary users of the application?	
5	Are there other applications that are dependent on the application?	

Figure 43: Business Questions

Infrastructure

#	Questions	Answer
1	How do users access the application (e.g., via web site)?	
2	If the application web-based, what java version does the application require?	
3	Does the application use an application server? If so what is application server (including version)?	
4	Does the application use a web server, if so what web server (including version) does the application use?	
5	Where is the user information stored (e.g., AD, LDAP, Database –please also specify version) for the application?	
6	Which core IT systems are involved with the application? (e.g., existing legacy systems, applications, databases)	

#	Questions	Answer
7	Are there any future platform migrations/rollouts or upgrades currently being planned?	
8	When accessing the application, do users have to pass through any firewalls?	
9	Does the application support self-registration or self-service (can the user request application through a self-service mechanism)?	
10	How many users does the application support in total (including concurrent users)?	
11	What are the applications high availability, business continuity, and disaster recovery requirements and architecture (e.g., session state, failover, hot spare)?	
12	Where is the physical location for the server that hosts the application?	
13	Besides people-oriented data, will other types of data need to be stored (e.g., devices, resources, location-related, organization-related)?	

Figure 44: Infrastructure Questions

Security

#	Questions	Answer
1	How are privileged users handled in the application?	
2	Does the application use role-based security? If so, how does access vary by role?	
3	Does the application require the use of separate authorization policies for users, groups, roles, etc.?	
4	What are the application's current authentication and authorization process? (Does the user have to authenticate with username/password, digital certificate, two-factor, token etc.?)	
5	Does the application requires the use of "anonymous" users or "guest" users; that is, users that need access to non-sensitive or non-protected websites?	
6	What internal or external user data sources does the application authenticate against (if multiple, what is the order of priority)?	
7	How does the application gain access to these internal or external data sources?	
8	Does the application use a public key infrastructure? Digital certificates?	
9	Does the application have a time based security restriction? (e.g., User or group cannot access between the hours of 5 PM and 6 AM)	
10	What is the current security policy for this application with regards to passwords? (e.g., password length/allowed characters, reset interval, invalid attempt threshold)	
11	How are users passwords reset? On-Line? Via HelpDesk?	
12	Does the application support SSO?	
13	Can the application be configured to support SSO? Will it need additional development to support SSO, or will it apply for waiver?	
14	Does the application store data that is Classified or that is otherwise sensitive?	

Figure 45: Security Questions

Software Architecture

#	Questions	Answer
1	Is this application in-house built or off-the-shelf?	
2	Are there API's currently in place for this application?	
3	What languages are used to develop the application? (e.g., .NET, Java)	
4	Where is the source code for the application? If needed, where/how could we obtain the source code?	
5	Does the application use any external components or COTS software?	
6	If this is a COTS application, what customizations or modifications (if any) have been done?	
7	If this is a COTS application, is the current version supported and under maintenance? (and who owns the support agreement)?	
8	Does the application have any integration with other third-party applications (e.g., RSA SecurID Authentication Manager)?	

Figure 46: Software Architecture Questions

Account Linkage

#	Questions	Answer
1	Does this system have data easily accessible that can be used for consistent correlation back to the identity? For example, an EMPLOYEE ID stored on each account can be considered a good correlation key.	
2	Does this system have multiple accounts for a given person or identity? How many accounts might a given individual have?	
3	Are identities or accounts federated with other entities?	

Figure 47: Account Linkage Questions

Provisioning

#	Questions	Answer
1	Are there requirements for users to be able to request or modify access to this application? If so, what are the approval steps that need to be followed and which attributes need to be displayed?	
2	What documented workflows does this application service?	
3	What are the levels of approval for the application to be provisioned?	
4	Who manages provisioning endpoints?	
5	What is the policy for application attestation or recertification?	

Figure 48: Provisioning Questions

Privacy[61]

#	Questions	Answer
1	Are Social Security Numbers (SSNs) used or collected? If so, why are they used or collected?	
2	If SSNs are used, who is the legal authority for the collection of SSNs?	
3	What specific information about individuals could be collected, generated, or retained?	
4	If header or payload data is stored in the communication traffic log, what are the data elements stored?	

Figure 49: Privacy Questions

DATA CALL

Objective

The goal of this data call is to assist the ICAM project team to document the current state of ICAM at the agency. Along with the future state, this information will greatly assist in gap analysis and will help draft a roadmap that drives the ICAM program to a successful enterprise-level implementation. This information is critical to the development of a sound current state and it will dramatically reduce the number of assumptions in future state development.

Information Being Requested

The table below represents the type of information needed. It is a comprehensive but not exhaustive set of information being requested.

Information Requested	Description	Additional Notes
Concept of Operations (CONOPS)	A CONOPS is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system.	This also includes user based scenarios commonly referred to as "use cases."
Design Interface Document	The Design Interface presents the information required to define the interface(s) with other systems, as well as any rules for communicating with those interfacing systems.	
Requirements Document	This document identifies the business and technical capabilities and constraints of the solution/service to be developed.	There may be separate documents for business, functional, and/or technical requirements.
Solution Architecture	A document outlining the detailed Solution Architecture for the application or system. The document ensures that the Solution Architecture is in compliance with the agency enterprise architecture principles, best practices, and conceptual target application architectures.	

[61] Additional privacy questions can be found in FICAM Privacy Guidance for Trust Framework Assessors and Auditors.

Information Requested	Description	Additional Notes
Design Document	Design document describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces for the application/system.	This may include both system design and service design.
Security Document	A document describing the governance, risks, policies, and controls associated with the information security components of a system or application.	This may include a security plan, SOP or policy document.
Privacy Document	A document describing the privacy implications of the collection, use, and maintenance of information associated a system or application	This may include a System of Records Notice, Privacy Threshold Analysis and/or a Privacy Impact Assessment.
Network Diagram	A document that details network architecture including elements such as firewalls, routers, LAN/WAN details, etc.	

Figure 50: Information Being Requested

This page is intentionally left blank

Appendix E Security Impact Analysis Example

This impact analysis has been derived from an agency currently using this template. References to the particular agency have been removed; however, an agency is encouraged to use this template when performing its security impact analysis.

Background

Information systems are typically in constant states of change in response to new or enhanced hardware and software capability, patches for correcting errors to existing components, new security threats, and changing business functions, etc. Implementing information system changes can impact the security posture of the information system and thus should be considered as part of any well-defined change management process.

Purpose

The purpose of this document is to provide a rational and orderly process for ensuring that structural and configuration changes made to a department's information systems and information system environments, at the infrastructure and application layers alike, undergo an SIA. SIAs consider the impact system changes could have on the security posture of the information system.

Overview of the Process

When a change is identified as needing to take place in an IT system, an assessment of whether this change will alter or modify the system's security posture is a part of the change management process. The change management board should include an individual who can review the proposed change from a security perspective. This individual should be the existing system/application Information System Security Officer (ISSO) or security engineer for that system.

The initial step of the process is the identification that a change is needed. The individual responsible for security of the system should work with the system owner, the development community and information technology managers to understand the type of change required. Is the proposed change part of a normal release process, required maintenance or an emergency?

- **Risk Based.** A risk based approach is used to focus the SIA on protection areas that are most susceptible to increasing a system's risk exposure. Thus, the SIA is not designed to be a comprehensive review of all of the security controls protecting an IT asset or a replacement to the comprehensive security assessment performed as part of an Authorization-to-Operate assessment. The goal is to focus on security controls impacted by the proposed change and likely to have the greatest impact on the security posture of the applicable information system.
- **Types of Change.** Changes can be of different types. It is important that the scope and breadth of the SIA be commensurate with the change type and its potential impact on the information system's security posture. Change types vary from agency to agency; however, two common change types include normal releases, generally of a maintenance nature, and emergency. The change type will also drive the speed with which the analysis must take place. For example, an emergency change might undergo a lighter review up front and more analysis after the event. On the other hand, a scheduled update would include an SIA as part of its change management routine.

The individual reviewing for security impacts needs to understand the nature and scope of the change. Generally, you will need to understand what component is being changed and how the component is being changed. Changes can include modifications to a system's configurations, changes to the hardware, operating platform or software, movement of a system physically, etc.

- **Understanding Vulnerabilities.** Changes can inadvertently create or open weaknesses in a system. It is important to protect against this potential. If the change involves Commercial Off-The-Shelf (COTS) hardware or software products, identifying vulnerabilities may require a search of the National Vulnerability Database (NVD) or other credible sources so that the vulnerabilities may be addressed or removed prior to the change going forward. Other credible sources include the US Computer Emergency Readiness Team (US-CERT), and an agency's Office of Information Technology Security.

The individual reviewing for security impacts needs to assess whether the proposed change will alter the overall risk posture of the information system. The reviewer can do this by reviewing the likelihood that a system change will alter the implementation of a specific implemented security control and determine the scope of the control modification.

- **Assessing Risks.** Once the SIA has identified a change to a security control, an assessment is needed to determine the impact of the change to the system's security posture. Changes by themselves do not change security postures and some changes have minimal impacts so that no further work or thought is needed. In other cases, the change may introduce significant risks thus meriting additional security safeguards and countermeasures to reduce that risk.[62]

Conducting and Recording Security Impact Analysis Results

The SIA is broken into two Phases.

1. Phase I walks the assessor through security controls and asks the assessor to decide if the change would affect the implementation of the security control and the severity of the impact. Phase I should take place prior to the change taking place.
2. Phase II asks the assessor to document whether any testing is needed to ensure that the assessment values of Phase I are accurate. System testing generally takes place prior to the change going into production, but Phase II can take place after the change.

This document provides a template Figure 51 the assessor can use to record his/her findings. A completed template can be saved as part of the system's formal security documentation. (Control CM-4: Security Impact Analysis)

Documenting changes: If a system change modifies how a security control is implemented, that change needs to be documented in the system's applicable system security plan. Depending on the agency this information may also have to be replicated in other agency-wide systems.

SIA Date and Analysts: Capture the names, organizational affiliation and title of the individuals conducting the Security Impact Analysis.

[62] Severity values of high equal a significant change.

Completing the SIA Template

1. Enter System Name if not filled automatically
2. Enter System Code if not filled automatically
3. Enter System Categorization if not filled automatically
4. Enter System Type: Hosting Infrastructure or Application
5. Describe the System Change or reference where a reviewer would find a description of the system change
6. Select the Change Type: Normal Release or Emergency
7. Review sources of known vulnerabilities to confirm that the proposed change will not introduce unexpected or unintentional vulnerabilities.
8. Review of the Impact of the Proposed Change on the security controls implemented on the system.
    a. Phase I

       Go through each of the NIST 800-53 controls and determine if the proposed change will affect the implementation of the control in the system. If no change move on.

       If the change will affect the implementation of the security control, assess the impact of the change to the system's security posture in terms of severity. Four severity values are offered – H or High, M or Medium, L or Low, None

       1. High – substantial – completely changes the control implementation
       2. Medium – significant – a material or meaningful change to the control implementation
       3. Low – limited impact or limited change
       4. None – no impact whatsoever

    b. Phase II

       Follow up with System developers, program managers, system owners to ensure that the change is tested to ensure the security posture remains at an acceptable level of risk.
9. Work with System Owners and ISSOs to ensure that any changes to security controls are updated and documented.

1 System Name	**2** System Code	**3** System Categorization	**4** System Type: Hosting Infrastructure Application	
5 System Change Described: (brief description – no more than 250 words)				
6 System Change Type	Normal Release including Maintenance Releases		Emergency	
7 Vulnerabilities Found: Y/N Fixed: Y/N	**7a** Review NVD: http://nvd.nist.gov/ **7b** Agency Advisory Site **7c** DHS – US CERT: http://www.us-cert.gov/			
8 NIST 800-53 Control Family Questions		**Phase I:** Adverse Impact on security – Please note the Security Controls impacted and Impact level – H – M – L or None	**Phase II:** Post change review: security impact analysis is performed to ensure that the changes have been implemented as approved	
Controls Altered by the System change				
Access Control Family: Does the change modify, alter existing access control configuration or add new access control configurations to include privileges and methodologies – such as controlling permissions to files, directories, registry keys, and user activities such as restricting activities like modifying system logs or installing applications.	Y/N	**AC-3 Access Enforcement** **AC-4 Information Flow Enforcement** **AC-5 Separation of Duties** **AC-6 Least Privilege** **AC-7 Unsuccessful Login Attempts** **AC-11 Session Lock** **AC-14 Permitted Actions without Identification or Authentication** **AC-17 Remote Access** **AC-18 Wireless Access** **AC-20 Use of External Information Systems**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?

Audit and Accountability Family: Does the change modify, or add to the audit settings (e.g., capturing key events such as failures, logons, permission changes, unsuccessful file access, creation of users and objects, deletion and modification of system files, registry key and kernel changes).	Y/N	**AU-2 Auditable Events** **AU-3 Content of Audit Records** **AU-4 Audit Storage Capacity** **AU-5 Response to Audit Processing Failures** **AU-6 Audit Review, Analysis, and Reporting** **AU-7 Audit Reduction and Report Generation** **AU-8 Time Stamps** **AU-9 Protection of Audit Information**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?
Security Assessment and Authorization: Does the change require that the system be re-authorized? Does this meet the definition of a major change? It is at the discretion of the agency to define "major."	Y/N	**CA-3 Information System Connections** **CA-6 Security Authorization**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?
Configuration Management: Does the change modify, alter, update, or deviate from Department configuration standards and the system configuration management plan. Does the change any of the inventory components? If yes, has the Department's central information system repository – IAS – been updated with the information?	Y/N	**CM -2 Baseline Configuration** **CM-4 Security Impact Analysis** **CM-5 Access Restrictions for Change** **CM-6 Configuration Settings** **CM-7 Least Functionality** **CM-8 Information System Component Inventory** **CM-9 Configuration Management Plan**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?

Identification and Authentication: Does the change modify, alter, or add to the way users or devices are identified and authenticated? Identifier management includes changing default account names, determining length of time until inactive accounts are disabled, using unique user names and establishing user groups. Authentication controls include password length, use of special characters, minimum password age, multifactor authentication/use of tokens.	Y/N	**IA-2 Identification and Authentication (Organizational Users)** **IA-3 Device Identification and Authentication** **IA-4 Identifier Management** **IA-5 Authenticator Management** **IA-6 Authenticator Feedback** **IA-7 Cryptographic Module Authentication** **IA-8 Identification and Authentication (Non-Organizational Users)**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?
Media Protection: Does the changes modify, alter or add to the existing media or of the methods for storing, accessing, labeling, or sanitizing the existing media.	Y/N	**MP-2 Controlled Maintenance** **MP-3 Maintenance Tools** **MP-4 Non-Local Maintenance** **MP-5 Maintenance Personnel** **MP-6 Timely Maintenance**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?
Risk Assessment: Does the change decrease or elevate the categorization?	Y/N	**RA-2 Security Categorization**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?

System and Services Acquisition: Does the change require updates to system documentation or system development testing results?	Y/N	**SA-5 Information System Documentation** **SA-6 Software Usage Restrictions** **SA-7 User-Installed Software** **SA-9 External Information System Services** **SA-10 Developer Configuration Management** **SA-11 Developer Security Testing**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?
System and Communications Protection: Does the change modify, alter, or add to the network or system infrastructure (e.g., moving a system component physically or logically such as from behind the DMZ to in the DMZ)?	Y/N	**SC-2 Application Partitioning** **SC-3 Security Function Isolation** **SC-4 Information in Shared Resources** **SC-5 Denial of Service Protection** **SC-6 Resource Priority** **SC-7 Boundary Protection** **SC-8 Transmission Integrity** **SC-9 Transmission Confidentiality** **SC-10 Network Disconnect** **SC-12 Cryptographic Key Establishment and Management** **SC-13 Use of Cryptography** **SC-14 Public Access Protections** **SC-15 Collaborative Computing Devices** **SC-17 Public Key Infrastructure Certificates** **SC-18 Mobile Code** **SC-19 Voice Over Internet Protocol** **SC-20 Secure Name/Address Resolution Service (Authoritative Source)** **SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)** **SC-22 Architecture and Provisioning for Name/Address Resolution Service** **SC-23 Session Authenticity** **SC-28 Protection of Information at Rest**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?

System and Information Integrity: Does the change modify, alter or add to the network’s core security software needs or inventory? Changes can include applying vendor released patches in response to identified vulnerabilities and software updates.	Y/N	**SI-4 Information System Monitoring** **SI-7 Software and Information Integrity** **SI-9 Information Input Restrictions** **SI-10 Information Input Validation** **SI-11 Error Handling** **SI-12 Information Output Handling and Retention**	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?
Physical and Environment Protection: Is the information system moving to a new physical location?	Y/N	If yes, then all controls in this family must be reviewed.	H – M – L – None	Testing Performed: Y/N Testing method: Are results documented in the appropriate system?

Figure 51: Security Impact Analysis Template