- Introduction
- Cloud Identity Playbook
- Digital Autopen Playbook
- Digital Identity Risk Assessment Playbook
- Digitally Sign a Federal Register Notice
- Digitally Sign a Word Document
- Digital Worker Identity Playbook
- **Enterprise Single Sign-On Playbook**
  - Executive Summary
  - Centralize Application Access in Five Steps
  - Step 1. Gain Enterprise Support
  - Step 2. Plan Application Integration
  - Step 3. Prepare Service Integration
  - Step 4. Integrate Applications for Agency Use
  - Step 5. Federate Application Access
  - Appendix A. Troubleshooting Single Sign-On
- Phishing-Resistant Authenticator Playbook
- ICAM Governance Framework Version 1.0
- Identity Lifecycle Management Playbook
- Privileged Identity Playbook

Enterprise Single Sign-On Playbook

This playbook is a collaboration between the Identity, Credential, and Access Management Subcommittee of the Federal Chief Information Security Officer (CISO) Council and the General Services Administration Office of Government-wide Policy identity Assurance and Trusted Access Division

Date: November 16, 2021 - Version: 1.1 +

Executive Summary

The Enterprise Single Sign-On (SSO) Playbook is a practical guide to help federal agencies implement or modernize an SSO service for federal employee access to government applications. SSO is a component of Identity, Credential, and Access Management (ICAM) that agencies use to centralize access to applications. SSO enables end users to log in to multiple applications using extensible multi-factor authentication options. It also extends capabilities for applications that don't natively support multi-factor authentication. Other benefits of Enterprise SSO include:

1. Supporting IT modernization and cloud adoption projects - Provide a centralized access point to onboard on-premise and cloud applications.
2. Supporting remote workforce - Efficiently adapt to any location, various authenticators, and any device workforce.
3. Improving user experience - Streamline the user experience across all agency applications configured with the service.
4. Reducing identity-related help desk tickets - Allow automated provisioning and de-provisioning or self-service to reduce identity-related help desk tickets.
5. Improving security posture - Quickly resolve unauthorized access actions by centralizing authentication and monitoring activity.

Agencies can use this playbook to centralize application access for agency employees and contractors or federate access with other federal executive agencies. Updates to this playbook may include federating outside of the federal executive branch, but it is not included in this current version. This playbook outlines a five-step process to implement or modernize an Enterprise SSO service aligned with the Federal Identity, Credential, and Access Management (FICAM) architecture. This playbook is designed for identity program managers and enterprise and application architects interested in modernizing their access management systems for federal employee access to internal or external applications. Agencies are encouraged to tailor this playbook to fit their unique organizational structure, mission needs, and requirements. Other IT program participants, including program managers and application teams, may find value in incorporating this playbook approach in their planning.

Key Terms

These are key terms used throughout this document.

- Assertion - A statement from one agency resource to another that contains information about an identity.
- Assertion protocol - A data exchange format used to communicate authentication and authorization information between two agency resources.
- Authentication - How you verify the identity of someone or something trying to access an agency resource.
- Authorization - How you decide whether to allow someone to access an agency resource.
- Authenticator - Something an entity possesses and controls to authenticate their identity, such as a password, token, or code.
- Credential - An authenticator that is authoritatively bound to an identity.
- Public Cloud - A cloud infrastructure provisioned for open use by the general public. A public cloud exists on the premises of the cloud provider, owner, and operator, who may be a business, academic, or government organization, or some combination of the three. In the context of this playbook, "cloud" refers to a public cloud.
- Resource - A federal executive branch application or data repository.

Disclaimer

This playbook was developed by the General Services Administration Office of Government-wide Policy (GSA OGP) with input from federal IT practitioners. This document shouldn't be interpreted as official policy or mandated action, and doesn't provide authoritative definitions for IT terms. Instead, this playbook supplements existing federal IT policies and builds upon the Office of Management and Budget Memorandum 19-17 (OMB M-19-17), Enabling Mission Delivery through Improved Identity, Credential, and Access Management, as well as existing federal identity guidance and playbooks. Privileged user access (e.g., superusers, domain administrators) is out of scope for this playbook.

Centralize Application Access in Five Steps

An Enterprise SSO service centralizes authentication to applications across a federal agency. It provides a single portal or access point for multiple agency applications, consolidates authentication policies, and extends multi-factor authentication to applications that do not support it. This reduces the cost of identity-related help desk tickets and other tasks. In other words, an SSO service provides a centralized access method for agencies and potentially other federal agency applications. This playbook outlines five steps when implementing an Enterprise SSO service.

1. Gain enterprise support to implement a capability. If your agency is not already using an Enterprise SSO service, then it should be planned and funded first. Part of this is usually building a business case on the advantages and benefits and also identifying the target state after SSO implementation.
2. Plan application integration by performing an inventory and analysis of your applications. To perform an application inventory, collaborate across your agency, look at network logs and financial records, and talk with application owners. Once you create an application list, analyze it for common authentication characteristics, such as supported protocols and user communities.
3. Prepare SSO service integration by conducting an architecture review. Determine where agency user data is stored and how to connect it to the SSO service. Consider security integrations with Security Information and Event Management (SIEM) or other Continuous Diagnostics and Mitigation (CDM) tools.
4. Integrate applications with the SSO service. This usually follows a three-step process to configure, test, and release features to the user community.
5. Federate application access with other federal executive agency applications or other federal executive agency employees and contractors. Reuse existing federal employee or contractor identities, rather than repeat the process to establish a new identity for each application. Federating access includes establishing legal and technical agreements with partner organizations.

Step 1: Gain Enterprise Support

A centralized authentication service can benefit your entire agency, improving the end user experience and your agency's security posture. As you build a business case, capture the strategic benefits tied to specific business benefits. It's important to explain the purpose in the context of business objectives to gain support from agency executives and secure a funding source. Each strategic benefit may include a different agency program to collaborate with. Conducting a cost benefit analysis may help identify a funding source and gain further support. Federal cybersecurity requirements outlined in 6 USC 1523 reference each head of agency to implement a single sign-on trusted identity platform.

1.1 Understand the Fundamentals

SSO is a technology pattern used to centralize authentication among multiple applications. The data is exchanged using an assertion protocol. The two main types of assertion protocols used in SSO are Security Assertion Markup Language (SAML) and OpenID Connect (OIDC). Table 1 provides a brief description of each protocol. This playbook focuses primarily on SAML and OIDC because they're modern, vendor-neutral standards supported by almost all modern cloud applications. While this playbook does not describe how each protocol is designed, your SSO product or vendor should explain how their product supports each protocol.

Technical Standard	Description	More Information
SAML	An XML-based open standard for exchanging authentication and authorization data.	SAML 2.0 Technical Overview
OIDC	A JavaScript Object Notation (JSON)-based authentication layer of the OAuth 2.0 authorization protocol used to transmit basic user profile information.	Open ID Connect Foundation

SAML or OIDC?

Picking an assertion protocol is dependent on application support. If possible, defer to a more modern protocol such as OIDC if it's supported by the application. Assertion protocols are specific to web-based (on-premise and cloud) or mobile applications. Some SSO vendors can extend their products to integrate with workstations, Virtual Private Networks (VPN), Virtual Desktop Interfaces, or other on-premise applications and services.

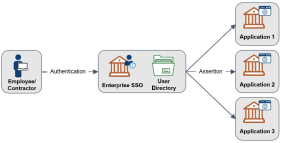


Figure 1: Enterprise SSO Overview

Table 2 provides descriptions and alternate terms that you might see for each actor in the transaction depicted in Figure 1.

Table 2. Enterprise SSO Overview

SSO Actor	Description	SAML Term	OIDC Term
Employee or Contractor	A person seeking to access an application.	User	User
Enterprise SSO Service	A service that conducts authentication of an employee or contractor. Referred to as the Identity Provider in NIST Special Publication 800-63.	Identity Provider (IdP)	OpenID Provider
Assertion	A digitally signed message from the service, using a specific protocol containing user data and access privileges, to a relying party.	SAML Assertion	ID Token, JSON Web Token
Application	A consumer of an assertion and may be referred to as a relying party or service provider. It may be located on an agency network or a cloud service.	Service Provider	Resource Provider

> ### Are we federated yet?
> Federation may have different meanings in different circles. In FICAM, federation is the sharing and acceptance of digital identities, attributes, and credentials managed by other agencies. SSO uses the same assertion protocols to share and accept digital identities with agencies and other federal applications.

1.2 Security Considerations

Applications rely on your Enterprise SSO to accurately and securely communicate and store user identity and attribute information. The centralized benefits of SSO can also increase the potential impact of security vulnerabilities. Table 3 highlights the most common SSO-specific risks that require mitigation strategies.

Table 3. Key Enterprise SSO Risks

SSO-Specific Risks	Recommendations
Session Key Browser Caching	Use encryption to secure connections and enforce time-restricted access and caching based on agency policies. Protection of assertion-bearing cookies is key to mitigating client browser attacks.
Signing Key Security	Refer to NIST Special Publication 800-63C Digital Identity Guidelines Federation and Assertions (PDF, June 2017) for specific guidance and considerations for the protection of your SSO's assertion signing key.
Assertion Validation	Each application validates that the assertions it receives are from a trusted source and appropriate for its sub-domain, functionality, and required attributes.

> ### Cyberattacks
> Targeted cyberattacks may pose a heightened risk to your agency's IT assets, such as enterprise directories, identity stores, and Enterprise SSO servers. Your SSO should be managed and monitored as part of your agency's cybersecurity program and in coordination with the DHS CDM initiative.

Users who are trained to enter their credentials without thinking can unintentionally supply them to a malicious credential prompt. Don't ask users to provide their credentials if the security posture of their sessions has not changed.

1.3 Build the Business Case

With any project, a business case is used to capture the strategic, business, and technical benefits from a project. Use examples in Table 4 below to craft your business case. The main benefits include:

Single Sign-On Strategic and Technical Benefits

Support IT Modernization and Cloud Adoption Projects −

- Efficiently extend your on-premise identity and access system to integrate cloud applications more rapidly.
- Facilitate use of modular and plug-and-play authentication options.
- Provide real-time data on application use.
- Provide a central user profile across all applications.
- Support centralized provisioning and de-provisioning.

Support Remote Workforce +

Improve User Experience +

Reduce Identity-Related Help Desk Tickets +

Centralize Monitoring and Security Controls +

✓ Best Practice - Building the Business Case

When building a business case, include qualitative aspects on how Enterprise SSO can improve user experience and security, a return on investment, and a cost-benefit analysis. Combining cost analysis (quantitative justification) and qualitative aspects may help obtain leadership support and funding.

Coordinate the business case development with your agency ICAM governance structure. The ICAM governance structure should oversee your ICAM projects and work streams and align ICAM services and management with your agency's mission. For ICAM oversight and program management examples, see the FICAM Program Management Guide.

1.4 Identify the Target State

Establish a realistic and achievable "to be" target state for your agency at key intervals (such as at one, three, and five years). Sometimes system impact level, access or credential requirements, or other factors can affect whether applications can integrate with your service. All applications are written differently, in different languages, at different times, for different purposes. Not all agency applications may support an assertion protocol. Your agency implementation should provide a range of compatible options, which will help realize the highest return on investment from the start.

Step 2: Plan Application Integration

Perform an inventory of your agency's applications, supported assertion protocols and provisioning capabilities, and user community.

2.1 Application Inventory and Identity Risk Analysis

Application inventory and identity risk analysis are critical implementations. As part of this application inventory, collaborate across your agency if a list doesn't already exist.

✓ Best Practice - Application Inventory Sources

Some agencies may not have a single authoritative source for application discovery or asset management. Your agency's FISMA asset and application inventories, DNS records, CDM asset management inventories, and network scan reports may assist in developing and maintaining an application inventory.

Your agency can group applications according to their major characteristics, similarities in use cases, design patterns, and technology stacks. Categorizing your application inventory based on these patterns help you to organize your pilot, integrations, and production releases. You may find efficiencies and scaling opportunities based on the below list. This list can also be used to prioritize application integration in step 4.

- Number of users per community of interest,
- Digital Identity Risk Assessment (DIRA) statement,
- Type of application (e.g., mobile, web, thick client),
- Business use cases (e.g., HR, financial, collaboration, productivity, and mission applications),
- Where the application resides (e.g., on-premise, cloud-based, or third-party hosted), or
- Budget cycle and financial priorities (e.g., cost savings).

For example, the Digital Identity Risk Assessment (DIRA) Playbook provides a process for identity risk analysis that includes both an application's level of data sensitivity and its user population (shown in Figure 2). The results are documented in a Digital Identity Assessment Statement (DIAS) which includes the identity, authenticator, and federal assurance level, which agencies can use and integrate as part of their overall Risk Management Framework (RMF) and FISMA processes.

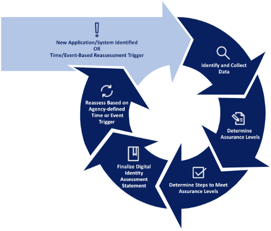

New Application/System Identified
OR
Time/Event-Based Reassessment Trigger
Identify and Collect Data
Determine Assurance Levels
Determine Steps to Meet Assurance Levels
Finalize Digital Identity Assessment Statement
Reassess Based on Agency-defined Time or Event Trigger

Figure 2: DIRA Process

✓ Best Practice - Digital Identity Risk Assessments

Your agency's DIRA process documents the minimum identity, authenticator, and federation level for a given application and assists with identifying similar applications.

2.2 Identify Assertion Protocol and Provisioning Support

After inventorying applications, document these application requirements:

- Assertion protocol supported,
- Attribute requirements such as username format,
- Provisioning support and the attribute requirements, and
- Endpoint or redirect Uniform Resource Locators (URLs).

Many of the items above can be automatically generated within either the SSO service or the application, but be prepared to configure them. Not every application supports an assertion protocol, but several web application vendors and development frameworks provide extensions that support SAML and OIDC.

Applications may also support automated account provisioning as part of the assertion protocol. Review application support and processes to perform automated provisioning.

2.3 User Population

Perform a high-level analysis to determine how your agency's enterprise users (employees and support contractors) currently perform their daily work. This provides a starting point for understanding your agency's user base and typical application use, including:

- Geographic locations (e.g., U.S. locations, overseas U.S. offices, international deployments),
- Types of work locations (e.g., fixed office, mobile, flexible, field-based),
- Modes of connectivity (e.g., high speed connections, low speed connections, intermittent connectivity, offline), and
- Types of credentials and assurance levels currently in use.

> ⚠ What about my authenticator?
>
> When you use centralized authentication, support for different authenticators depends on the SSO vendor, rather than the application. When reviewing products, consider support for different authenticators, such as Personal Identity Verification (PIV), Common Access Card (CAC), and non-PIV authenticators (e.g., one-time passwords (OTP) mobile applications, tokens, and mobile push notifications).

Step 3: Prepare Service Integration

The Enterprise SSO service serves as your primary authentication channel, but is integrated into your existing ICAM architecture. It may replace one or more existing authentication solutions. Conduct an architecture review and identify environmental considerations.

3.1 Conduct Architecture Review

Conduct an architecture review to determine what existing components you should integrate, such as:

- Authoritative source databases for user accounts (directories or databases),
- User provisioning and de-provisioning processes, or
- Integration with other security tools such as a SIEM tool.

In addition to system integration, the architecture review should include:

- System design, use cases, and security plan;
- Supported functionality, user interfaces, user support processes, administrative workflows; and
- Application level processes for new user community support.

Figure 3 provides a view of an example architecture, including where the Enterprise SSO is located within that architecture, and other potential integration points. For additional information related to the architecture, visit the FICAM Architecture Playbook Systems Component Examples.

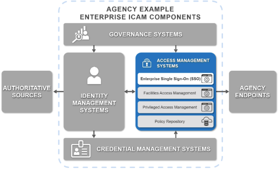

AGENCY EXAMPLE
ENTERPRISE ICAM COMPONENTS
GOVERNANCE SYSTEMS
AUTHORITATIVE SOURCES
IDENTITY MANAGEMENT SYSTEMS
ACCESS MANAGEMENT SYSTEMS
Enterprise Single Sign-On (SSO)
Facilities Access Management
Privileged Access Management
Policy Repository
AGENCY ENDPOINTS
CREDENTIAL MANAGEMENT SYSTEMS

Figure 3: Example System Components for an Agency Enterprise ICAM Program

> ℹ Identity Synchronization
>
> User data (e.g., identity) synchronization between the Enterprise SSO service and data repositories fall into two categories of one-way (unidirectional) or dual (bidirectional) syncs. One-way sync from the source directory to the service usually includes identity data and sometimes, passwords. Identify which service should be the authoritative source for data based on the sync method and plan accordingly.

3.2 Environmental Considerations

Agencies with applications that are accessible from a public cloud or use private or hybrid cloud services may need to plan for additional architecture and network considerations. Consider these questions in your planning:

- Is a VPN required to access the application or Enterprise SSO service?
- Where does a user need to be located (physically or virtually) to access an application?
- What type of device (Government Furnished Equipment (GFE), non-GFE, laptop, mobile) is required to access the application or Enterprise SSO service?
- Are there security, routing (e.g., multihoming), or functionality implications for connecting the applications or Enterprise SSO across networks or security zones?

Each of these factors can affect network routing, domain naming, and application of your agency's security policy.

Step 4: Integrate Applications for Agency Use

As discussed in step 2, application variability may require different models to integrate with an SSO service. Your agency implementation should provide a range of compatible options for application integration, allowing the highest return on investment.

The Enterprise SSO service operators and application owners should collaborate in the following areas:

- Establishing an assertion protocol between the service and the application;
- Enabling application registration, provisioning, and de-provisioning (manual or automated);
- Resolving user identities (directory synchronization exceptions) and other attributes,
- Identifying roles and responsibilities for operations and maintenance of the integration; and
- Updating end user support and help desk processes, where applicable.

4.1 Plan Application Integration

Applications can be grouped according to benefits from your business case in step 1 or similarities as described in step 2. Application integrations can be grouped and prioritized with these considerations:

- Highest use application or highest return on investment,
- Number of identity-related password reset or provisioning help desk tickets,
- Application location (cloud-hosted versus on-premise or vice versa),
- Security considerations for centrally monitoring access, and
- User community (federal employee, specific sub-agency, or office, etc.).

New applications follow a streamlined onboarding process with or without an early adopter or pilot phase. Migrating existing applications is generally more complex in terms of phasing and change management. Plan for phased migrations where possible, including incorporating testing and production pilot feedback prior to a full production release for existing agency applications, specifically:

- Configure the application with the service,
- Test the connection, and
- Release the app to the user community.

4.2 Configure, Test, and Release the Application

Application integration should follow a configure, test, and release pattern.

Configure

Application configuration is usually performed in one of two patterns.

SSO service-initiated - The service hosts a dashboard or a list of applications available to the user and is sometimes referred to as Identity Provider or IdP Initiated. The transaction includes the following steps:

1. A user attempts to access the SSO service directly.
2. The user authenticates to the SSO service and selects an application from a dashboard or list.
3. The SSO service generates a signed assertion and the user is redirected to the application.

Application-initiated - The application redirects the user to the SSO service portal. This is sometimes referred to as Service Provider or SP-initiated.

1. A user attempts to access the application directly.
2. The user is redirected to the SSO service.
3. The user authenticates to the SSO service.
4. The SSO service generates a signed assertion and the user is redirected back to the application.

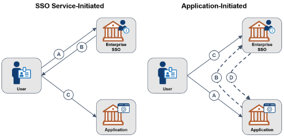


Figure 4: SSO-Initiated vs Application-Initiated Models

Configuring the application usually involves sharing configuration data between the SSO service and the application. What and how information is shared is dependent on the assertion protocol, but most SSO vendors have comprehensive configuration documentation. Every application may have a unique process to enable SSO. Even though the application may be unique, the assertion protocol is standardized.

- SAML - Configuration usually entails sharing a metadata file of connection information between the SSO service and the application. This creates the secure connection and ability to share identity information.
- OIDC - Configuration is usually more automated. It usually entails logging into the application and authorizing the connection to the SSO service. It may also follow a similar metadata process to SAML.

Although SAML and OIDC may require some manual configuration, it's usually a short and straightforward process. Part of the application configuration includes the format of identity attribute sharing. During the application inventory, document the application username format. It may be different from what is used to authenticate to the SSO service. In step 2, you determined whether the application can support account provisioning within the assertion protocol. As part of the application configuration, you can set other user attributes required to establish an application account.

Unique Identifiers

SSO vendors rely on the use of a unique identifier (e.g., an email, an agency-defined identifier). This is usually the username used to access the SSO service. Application-specific username formats may also be supported. For example, jane.doe@agency.gov is used to log into the SSO service and then, the service may convert that to an application specific name such as janedoe01.

Test

Once an application is configured, it should go through a test cycle to ensure it functions properly and maintains or improves the user experience. Testing may include:

- Creating a test account in the SSO service,
- Testing a service or application initiated login pattern, or
- If supported, test provisioning from the service to the application.

Release

Once an application is configured and tested, it can be released to the user community. This should come with an agency communication announcing the use of an SSO service, if not already in use. This may also include training or other communications to help user adoption and experience.

Step 5. Federate Application Access

In FICAM, federation is the sharing and acceptance of digital identities, attributes, and credentials managed by other agencies. Prior to this step, it's very possible many applications are individually configured to directly manage or accept a wide variety of credentials or authenticators, known as direct enablement. This model allows applications to support disparate user populations, but is both time consuming and resource intensive to maintain. Direct enablement and local credential management increase the risks associated with account de-provisioning. For instance, a user may have been separated from their role or organization, but accounts and credentials (e.g., local username/password) in individual applications may be unknowingly left active.

Enterprise SSO limits the complexity and risks of direct credential enablement. With SSO-based identity federation, authentication transactions are standardized regardless of the credentials or authenticators, and user management activities can be consolidated under the Enterprise SSO.

Table 5 provides a comparison of some benefits and drawbacks of federation and direct enablement.

Federation vs Direct Enablement Comparison

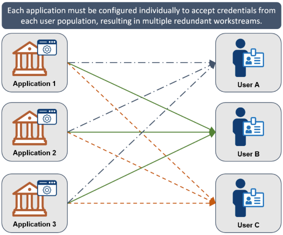
Configuration Management −

SSO with Federation Benefits	Direct Enablement Drawbacks
• Only the SSO service needs to be updated to accept new credentials or authenticators. • Maintenance changes (e.g., trust store management or revocation checking) can be consolidated at the Enterprise SSO. • Unique user identification can be standardized across an enterprise and more easily extended for new user populations.	• Applications need to be individually updated to accept new credentials or authenticators. • Each application must make needed technical configuration changes to maintain interoperability. • Each application needs to plan for and implement a unique identification schema (which may not be reusable in other systems).

Security and Accreditation +

Help Desk Support +

Figure 5 highlights the potentially redundant effort for each application to accept users and/or credentials from different groups using the direct enablement method. Figure 6 depicts the reduced complexity of an identity federation.



Each application must be configured individually to accept credentials from each user population, resulting in multiple redundant workstreams.

Figure 5: Direct Enablement with Overlapping Configuration Efforts

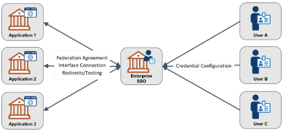


Figure 6: Identity Federation, Streamlined Configuration

After step 4, an agency may consider federating their SSO service and applications with other agencies. This comes in two patterns:

1. Allow access to agency applications from other federal agency SSO services.
2. Federate your agency's SSO service with other federal agency applications.

Inter-agency federations, access between and among U.S. federal executive agencies, assumes that agencies are building on or have completed steps 1 through 4. Inter-agency federation provides agencies with a common trust and technology infrastructure that accepts existing agency enterprise identities. It also minimizes the redundant collection of identity data and issuance of duplicate user identities. The justification for granting access to another agency's users is based primarily on the agency's mission, business functions, and services:

- Have a government-wide user community – including information sharing and knowledge repositories, human resources, training, financial, and personnel security services.
- Provide as shared or managed services – supporting agencies as IT service subscribers.
- Support specific mission and business functions – with users from two or more agencies collaborating together.

⚠ Federal Workforce Identities

The scope of this playbook is federal enterprise user access to federal enterprise applications. An agency may have other user communities that include state, or local government users, mission partners, or citizens.

5.1 Planning Considerations

From an enterprise SSO perspective, integrating with another agency's application or enterprise SSO service is very similar to application onboarding. It follows a similar pattern in that it's either a service or application initiated login attempt using an assertion protocol. Additional planning considerations include:

- Resolve user identities and other attributes required by the application.
- Store and share interface control or other agreements between agencies including protocol and attributes at a federation assurance level identified through a DIRA or in a DIAS.

Each application integration should follow a similar configure, test, and release pattern:

- Redirect link to agency identity provider or a "log in with my agency enterprise SSO" button on the application login page.
- Test the new implementation.
- Plan for changes to the system over time.
- Schedule a phased capability rollout to user communities, if applicable.
- Iterate on your system and processes regularly.

5.2 Agreements/Building Trust between Federal Executive Agencies

Technical trust is established between agencies participating in an identity federation through the use of agreed-upon assertion protocols and recorded in interface control documents. However, a business and mission-level agreement is frequently required to document inter-agency agreements in the form of an agency CIO-signed federation agreement.

Agency mission areas may submit documentation of their assurance level and attribute requirements with the federation agreement from the enterprise. These may be captured in existing agency questionnaires as a "customer journey map" or preferably using the DIRA process which includes standardized processes and procedures to identify an identity, authenticator, and federal levels mapped to [SP 800-63-3].

This document may be incorporated as an annex or appendix to the Authority to Operate (ATO) for each of the participating IT applications and identity providers.

Appendix A. Troubleshooting Single Sign-On

Software issues or changes in the environment can cause a working configuration to stop working. When this occurs, SSO administrators can use the following steps to identify the cause and restore access.

1. Check SSO and application logs

Authentication errors usually create a log entry in the SSO or the application. This error could help identify a root cause, but oftentimes errors may not be specific or clear. Since SSO often involves authentication to external applications, this may require some coordination with other entities.

2. Check network routing

Sometimes it's the simple things. If users are reporting that they can't access an application, make sure that there isn't a network outage or a firewall issue.

3. Test a known good app

When a user reports that they are unable to access an application, they may blame the SSO infrastructure when the problem actually lies in the end application. SSO administrators should try an app that is known to work in order to distinguish app issues from SSO infrastructure issues. Ideally, the administrator team should have a sample application which will allow them, and the user to validate SSO access.

4. Check Certificates

For signed assertions, an expired certificate can cause the assertions to not be trusted. If access is failing for an application or a set of applications, confirm that the certificate is not expired. This may be recorded as an error by the end applications.

5. Check application configuration

Changes in the configuration of the application assertion receiving and processing are a frequent error cause. This may be due to an application upgrade, or to an inadvertent change by an application administrator. This configuration error should show up in the application logs, but the errors may not be very clear.

6. Collect assertion data and use assertion analysis tools

Finally, if there are no other apparent issues, it may be necessary to inspect the assertion for encoding or other errors. While these errors are not common, they do occur and can result in very subtle errors that are difficult to troubleshoot.

IDManagement.gov
An official website of the U.S. General Services Administration

Looking for U.S. government information and services? **Visit USA.gov**
This site is a collaboration between GSA and the Federal CIO Council. It is managed by the Identity Assurance and Trusted Access Division in the GSA Office of Government-wide Policy.