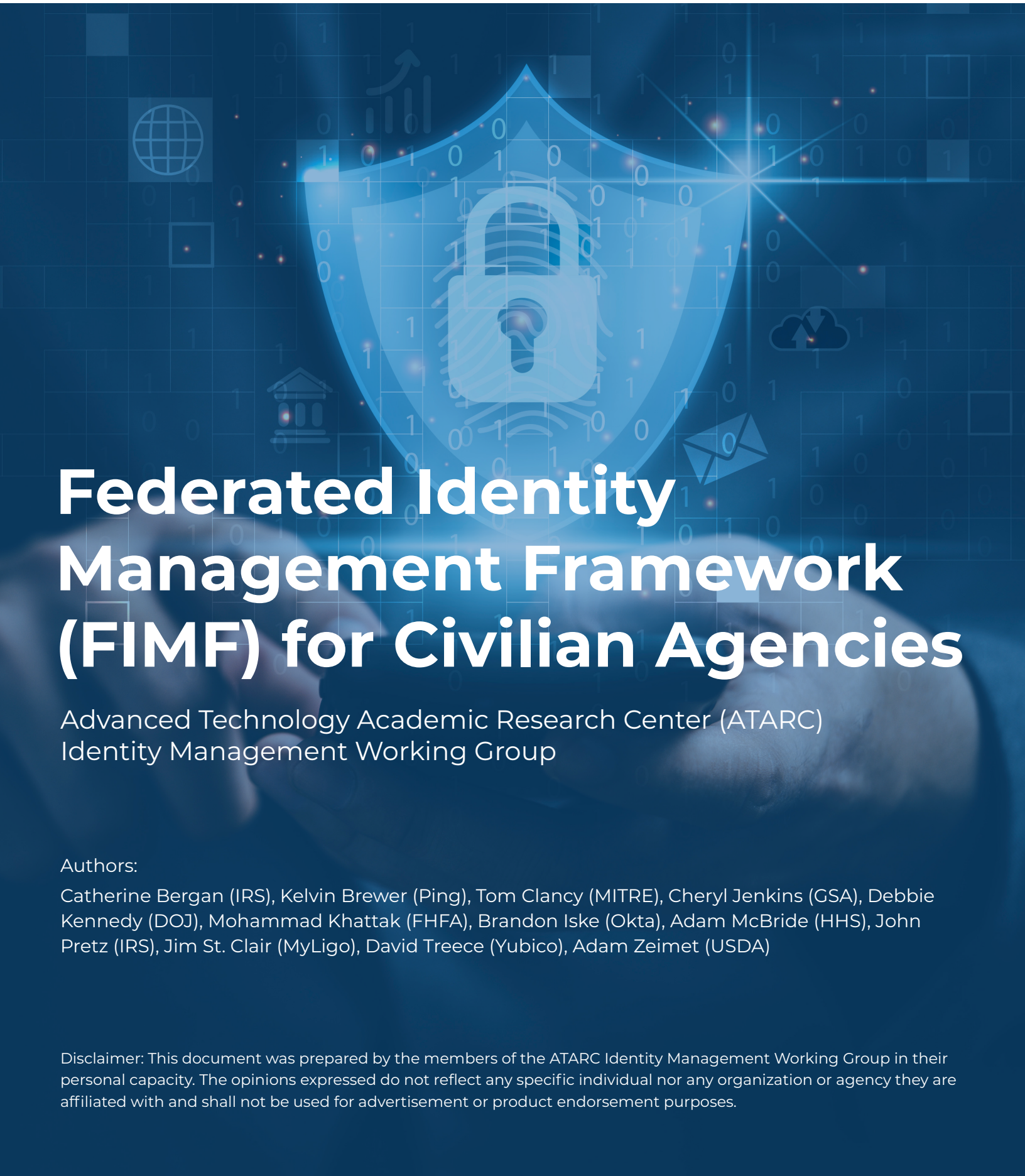


Federated Identity Management Framework (FIMF) for Civilian Agencies

Advanced Technology Academic Research Center (ATARC)
Identity Management Working Group

Authors:

Catherine Bergan (IRS), Kelvin Brewer (Ping), Tom Clancy (MITRE), Cheryl Jenkins (GSA), Debbie Kennedy (DOJ), Mohammad Khattak (FHFA), Brandon Iske (Okta), Adam McBride (HHS), John Pretz (IRS), Jim St. Clair (MyLigo), David Treece (Yubico), Adam Zeimet (USDA)

CONTENTS

EXECUTIVE SUMMARY

An identity federation occurs according to a shared responsibility model. The US Government has determined the need to leverage identity federation to achieve strategic outcomes of effectiveness and efficiency among federal agencies and in conjunction with mission partners. This framework describes how federal agencies will federate the use of identity and use across the Federal Government.

The federal government has made significant strides in maturing its authentication methods for access to enterprise platforms and applications and arguably maintains one of the largest federated identity networks in the world. These methods began with passwords and have evolved into single sign-on capabilities that enable employees to access multiple applications within the same enterprise using a single set of credentials. However, expanding authentication capabilities beyond the enterprise for agencies to transact business with other agencies, business partners, and citizens presents challenges due to divergent interpretations of policy and technical guidance. This has led to a lack of uniform trust, resulting in redundant and duplicative

EXECUTIVE SUMMARY

processes for identity verification and validation, culminating in unnecessary expenditures and overcollection of Personally Identifiable Information (PII). Moreover, this challenge impedes modernization requirements directed in [M-19-17] by the Office of Management and Budget, aimed at advancing the technical approach for managing identities and improving digital interactions with the American public. This concern was reiterated by agencies during the 2024 FICAM Day, co-hosted by the General Services Administration (GSA) and the Advanced Technology Academic Research Center (ATARC). According to the proceedings, there was a consensus among agencies to develop a Federated Identity Management Framework (hereafter referenced FIMF) for facilitating cross-entity trust (i.e., government-to-government, government-to-business, and government-to-citizen). This document serves as guidance with an initial focus on government-to-government trust and aligns with [800-63C], the [Federal Zero Trust Strategy], and the ICAM common business requirements.

Within this framework, there are two principal models for federation:

- A hub-and-spoke federation, in which a centrally-operated hub facilitates the federation of identity providers (IDPs) for access by users supported by the federated IdPs to access resources supported by other IdPs.

- A federation broker, in which a single IdP provides services directly to applications on behalf of additional IdPs.

This framework anticipates the need to apply both patterns simultaneously to meet federal business and mission needs, internally and externally. The intention is to develop an accompanying technical document to determine which model to use.

PURPOSE AND EXPECTED OUTCOMES

The objective of this proposed Trust Framework guidance is to establish a robust governance and operating structure primarily focused on enhancing government-to-government (G2G) interactions in cross-agency application sharing with employees and contractors using one government issued Personal Identity Verification (PIV) card or alternative issued token. While this iteration of the FIMF establishes the foundation for cross-agency trust, it accommodates broader engagements with enterprise partners and citizens.

Outcome #1 – Facilitate secure and efficient identity verification and credential sharing streamline processes

Outcome #2 – Reduce redundancy in identity management and ensure compliance with relevant laws and regulations

Outcome #3 – Fostering mutual trust among participating agencies

It is envisioned that a cohesive identity management ecosystem will evolve that enhances collaboration and improves service delivery across all levels of government.

Keywords: Federation, Hub-and-spoke, broker, trust framework, trust agreement, interagency, mission partner

FEDERATED IDENTITY MANAGEMENT FRAMEWORK (FIMF) FOR CIVILIAN AGENCIES

From the Federal ICAM Day proceedings, it became evident that federal agencies are encumbered by redundant and duplicative HSPD-12 processes for identity verification and validation. The onboarding procedures across agencies exhibit significant variability, resulting in diverse process hooks and workflows that complicate management efforts. Additionally, disparate policies, regulations, and programs delineate the sequence and conditions under which credentials are issued to personnel, as well as the information systems that underpin personnel data management. This inefficiency not only incurs unnecessary expenditures but also leads to the overcollection of Personally Identifiable Information (PII).

Furthermore, the current infrastructure (e.g., current agency-specific identity systems) does not adequately reflect the principles of Zero Trust Architecture (ZTA) in managing identity. In this context, it is imperative to adopt a federated identity management framework that enhances interoperability and standardization across agencies. The absence of a federated identity management framework presents significant challenges, including inconsistent policies, lack of governance structures, and incongruent technical interoperability capability across agency environments. These challenges can hinder collaboration and complicate the seamless sharing of credentials and data. To mitigate redundancy in the issuance of PIV cards and promote the use of one PIV card for cross-agency application sharing, various methodologies may be employed; resulting in complexities if not underpinned by a framework that aligns with common ICAM business standards.

This federated framework encompasses shared governance structures, unified standards, trust agreements, and collaborative protocols that facilitate seamless credentialing processes and data sharing while ensuring compliance with federal mandates.

By embracing a federated approach to Identity Management and Credential Management (ICAM) functions, agencies can better align their practices with a cohesive strategy that promotes secure and efficient identity verification. As we advance, this federated paradigm should be integral to the development of ICAM common business standards and capabilities in cyber security, information technology service, and Human Capital Management federal functions.

SCOPE

The initial scope of FIMF and the defined governance and operating structure is trust framework alignment and technical interoperability for federal civilian government-to-government (G2G) interactions, establishing a solid foundation for future expansions into broader engagements, including high-level Citizen-to-Government (C2G) and Business-to-Government (B2G). requiring access to shared applications within the federation. Though much of the paper can be leveraged for DoD and state agencies, the scope has been kept narrow to ensure it can be actionable. Specific guidance focusing on their needs could be addressed in future papers. Additionally this paper will not address non-human entity accounts. This is a growing and important area but has unique use cases and goes beyond the scope of this paper.

The framework advances policy alignment and technical interoperability of identity providers, which may include all aspects of identity management, credential issuance, access control, data privacy, and security measures necessary to maintain the integrity and confidentiality of sensitive information for G2G interactions. An identity provider may organically support identity provider functionality or compose IdP functions from organic or third-party identity provider services. The constituent services within an IdP include robust identity verification processes, secure communication channels, and comprehensive data protection strategies to mitigate risks associated with external access.

APPLICABILITY

The provisions of this trust framework are mandatory for all personnel involved in identity and access management processes. This includes agency heads, IT security officers, users, and any third-party entities interacting with the federation's resources. All stakeholders are required to adhere to the principles outlined in this framework to ensure a secure and trusted environment for information sharing and collaboration among government agencies.

Third-party service providers must implement rigorous compliance mechanisms to align with the Trust Framework's standards. This includes undergoing regular security assessments, maintaining certifications that demonstrate adherence to federal guidelines, and actively participating in continuous monitoring and reporting processes. By fostering a culture of accountability and transparency, the framework aims to ensure that all interactions—whether G2G, C2G, or B2G—are conducted within a secure and trustworthy ecosystem.

TARGET AUDIENCES

The target audience encompasses a diverse range of stakeholders, including IT administrators, security professionals, compliance officers, and end-users. This group is integral to the successful implementation and maintenance of identity management systems, as they each play a critical role in ensuring secure access to information and resources. By addressing the unique needs and concerns of these stakeholders, we aim to foster a collaborative environment that enhances security protocols, streamlines user access, and ensures compliance with regulatory standards, ultimately contributing to a more secure and efficient organizational framework.

This framework applies to all government agencies participating in the FIMF and encompasses all employees, contractors, and third-party service providers. Third-party service providers play a critical role in this Trust Framework, as they often supply specialized capabilities, technologies, and services that enhance the overall efficiency and effectiveness of identity management and access control processes. These providers may include cloud service platforms, identity verification services, data analytics firms, and cybersecurity solutions that support government operations. The framework ensures that these third-party entities adhere to stringent security protocols and ZTA compliance measures, safeguarding sensitive information and maintaining the integrity of G2G interactions.

ROLES AND RESPONSIBILITIES

FRAMEWORK MANAGERS

Federal agency representatives who establish oversight mechanisms to ensure ongoing compliance with the trust framework. Specific activities are listed below, but not limited to:

a. Approves trust agreements

b. Resolves incongruity in the framework

c. Establishes and directs working groups as deemed necessary

d. Establishes security criteria for federation in alignment with NIST standards and guidance

e. Identifies opportunities and shared ICAM solutions to expand the federation community

f. Posts approved federation practice statements and trust agreements to a website

ROLES AND RESPONSIBILITIES

TECHNICAL MANAGERS

Federal agencies that provide and manages a federation solution that has the following minimum capability:

a. Registers federation members

b. Establishes and maintains discovery mechanism to determine which environment and account the user is accessing

c. Prevents cybersecurity incidents by blocking unauthorized members from joining the federation or accessing shared resources

d. Validates and monitors federation membership to ensure compliance with this framework

e. Provides a standard Application Programming Interface (API) and protocols to ensure interoperability among federation members.

f. Reports cybersecurity attacks and compromise to the Framework Manager and in the Cybersecurity and Infrastructure Security Agency's Incident Reporting System.

SECURITY MANAGERS

Federal agencies that provide and manages a federation solution that has the following minimum capability:

a. Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.

b. Risk Management Framework (RMF) requirements

c. Cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

d. Personally Identifiable Information (PII) data security standards.

ROLES AND RESPONSIBILITIES

FEDERATED IDENTITY MANAGEMENT FRAMEWORK (FIMF) WORKING GROUP

The Federated Identity Management Framework Working Group (FIMFWG) serves as the principal cross-agency coordinating body for developing, implementing, and maintaining interoperable identity federation standards and practices between federal agencies and their partners. The FIMFWG operates at an executive level, ensuring alignment with federal policies, security requirements, and technological advancements while providing strategic direction for identity federation initiatives. The FIMFWG will also serve as the independent verification and validation of Identity Providers (IdP) capacity to deliver federated identity management services. The FIMFWG would have the following responsibilities:

a. Registration, Adjudication and Approval of Identity Providers to the FIMF registry

b. Maintain and Manage Technical Standards

c. Recommend Policy and Governance

d. Conduction Operations for participating agencies

e. Address Security and Risks identified through FIMFWG meetings

Success of the FIMFWG will be gauged through measurement of the following:

a. Usage of approved FIMF frameworks across federal agencies

b. Reduction in implementation time for new identity federation initiatives

c. Improved security posture related to identity federation

d. Reduction in costs associated with identity federation

e. Increased interoperability between federal agencies and partners

f. Positive feedback from stakeholders

ROLES AND RESPONSIBILITIES

IDENTITY PROVIDERS

An identity provider is a system or service responsible for managing and verifying a federation member's digital identity. These requirements apply to identity providers that will implement interagency or external federations. They are responsible for the following activities, but not limited to:

a. Designation of Federation Point-Of-Contact (POC) to serve in the capacity of an observer with the Framework Managers to provide input to oversight activities and decisions, as well as with FIMFWG to report compliance and operational status of federation capabilities.

b. Designation of a Federation POC to report compliance and operational status of Federation

c. Documents the practices, procedures, and processes to manage and maintain their Federated Identity system or service in accordance with a federated practice statement (FPS)

d. Submits their federation practice statement to the FIMFWG for review and Federated Managers approval.

e. Submit to third-party assessments and audits or perform internal assessments and audits of their operations as required by the specific trust agreements, or at least annually. Submit results to the FIMFWG for review and approval. Assessments and audits should strive for automation that provides continuous and near real time data.

f. Ensures the minimum metadata are included in any assertions (or tokens).

- Subject: Identifier for the party the assertion is about
- Issuer: IdP Identifier issuing the assertion
- Audience: Identifier for RP (assertion consumer)
- Issuance: assertion timestamp
- Expiration: time assertion expires and should no longer be accepted by RP
- Identifier: Value uniquely identifying the assertion

ROLES AND RESPONSIBILITIES

- Signature: Digital signature of assertion including public key of IdP (for certificate-based authentication)
- Authentication time: Timestamp when IdP verified presence of subscriber at the IdP through a primary authentication event.
- Attribute metadata (see NIST Interagency or Internal Reports (NISTIR) 8112)

g. Minimizes storage and transmission of PII. Pass identity attributes only to authorized resource servers using an identity API rather than including them in assertions or tokens. Provides written notice to the Federated Managers, no less than 60 days prior to planned changes in assertions. If operational issues or security concerns require a federation member to take immediate action, notice shall be provided to the Federated Managers within one (1) hour.

h. Employs appropriately tailored security controls (to include control enhancements) from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard for all federation capabilities.

i. Supports contested, degraded, or operationally limited environments and provides details on this support in their FPS.

FEDERATION SECURITY, AUDIT AND TECHNICAL REQUIRE-MENTS

The Federated Identity Management Framework (FIMF) will consist of the following components:

1. Identity Provider (IdP)
2. Entity Identity Attributes
3. Reauthentication and Session
4. Federation Entity Identities

All components must ensure security compliance to the following requirements:

a. Have or obtain a signed Authority to Operate

b. Meet Security controls based on FIPS-199 categorization. Note: security control implementation may be subject to tailoring for certain federations or entity categories.

c. Compliance Data Protection Protocols – Security measures to ensure that access to sensitive information is restricted to authorized personnel only.

d. Determine if the residual security and privacy risk from operating a system or using a system, service, or application from an external provider is acceptable.

e. Establish acceptable limits for the software application, network, or system.

f. Incident Response Plan

g. Configuration management Plan

h. Security Auditing and Monitoring

All components must comply with the following audit and compliance requirements:

Regular Audits: Conduct periodic audits of identity and access management practices to ensure adherence to the trust framework.

FEDERATION COMPONENTS

IDENTITY PROVIDER COMPONENT

Each IdP will meet the following features:

Interoperability: Commitment to implementing security and interoperability profiles of standardized protocols (e.g., SAML, OpenID Connect/OAuth).

Identity Assurance: The security level regarding the federated framework's Identity Assurance is structured through a tiered approach that aligns identity verification processes with the sensitivity of the information being accessed. This model consists of three baseline Identity Assurance Levels (IAL), Authenticator Assurance Levels (AAL), and Federation Assurance Levels (FAL), as defined in NIST SP 800-63-3, each designed to mitigate risks based on the required security posture.

Organizations, applications, service providers, and identity providers tailor baseline security requirements for each assurance level as required within the Digital Identity Risk Assessment (DIRA) process defined by NIST. Typical examples of US Government tailoring include: a requirement for liveness checking during remote proofing at IAL2 and including the requirement for phishing resistance at AAL2 on a FIPS validated authenticator.

IdPs must be able to receive authentication requests that include specific identity assurance requirements (xALs) and MUST include xALs met by authentication ceremonies in assertions or tokens provided to applications they support. Doing so supports the requirements of PIV federation in FIPS-201 and the requirement for collection of logs defined by OMB M-21-31.

FEDERATION COMPONENTS

- **IAL1 (Lowest Identity Assurance):** At this level, there is no requirement to link the applicant to a specific real-life identity. Self-asserted attributes or basic identifiers are sufficient. This level is suitable for accessing non-sensitive information, where the risk of identity fraud is low.
- **IAL2 (Moderate Identity Assurance):** This level requires evidence of identity, such as government-issued identification, validated through remote or in-person identity proofing processes. It provides moderate confidence in the identity and is appropriate for moderate-risk environments.
- **IAL3 (High Identity Assurance):** IAL3 requires stronger identity proofing, including in-person verification and biometric data collection where applicable. This level ensures high confidence in the individual's identity and is essential for accessing sensitive or high-risk information.
- **AAL1 (Lowest Authenticator Assurance):** Requires single-factor authentication (e.g., a password or PIN). This level provides basic protection against unauthorized access and is suitable for low-risk scenarios.
- **AAL2 (Moderate Authenticator Assurance):** Requires multi-factor authentication (MFA), such as a combination of something the user knows (e.g., password) and something the user has (e.g., a token or mobile device). This level offers greater assurance for moderate-risk environments.
- **AAL3 (High Authenticator Assurance):** Requires MFA with a hardware-based authenticator (e.g., a PIV card or cryptographic device) and strong resistance to phishing or replay attacks. This level is critical for high-risk systems.
- **FAL1 (Lowest Federation Assurance):** Allows federated identity assertions with minimal security requirements, such as self-signed assertions. Suitable for low-risk federated interactions.
- **FAL2 (Moderate Federation Assurance):**Requires signed assertions and encrypted communication between the IdP and relying party (RP), ensuring trust in moderate-risk federated scenarios.
- **FAL3 (High Federation Assurance):** Requires strong cryptographic protections, mutual authentication between IdP and RP, and resistance to man-in-the-middle attacks. Essential for high-risk federated interactions.

FEDERATION COMPONENTS

Overall, the federated framework's Identity Assurance, Authenticator Assurance, and Federation Assurance effectively balance security needs with user accessibility, ensuring that the appropriate levels of identity proofing, authentication, and federation trust are applied according to the sensitivity of the information involved. This structured approach helps to mitigate risks and enhance the overall security posture of government agencies.

Credential Lifecycle Management: Centralized processes for credential issuance, management, and revocation, ensuring integrity and trust. IdPs typically implement the lifecycle of user credentials. IdPs that do must implement "coupling" for the user's subscriber account at the IdP to the user's PIV identity account, or master user record entry, at the user's home agency. Methods for coupling subscriber and identity accounts are described in NIST SP 800-217 and NIST SP 800-157r1 drafts and include the use of a provisioning protocol.

Authorization: IdPs may support one or more authorization methods and contexts used by protected resources. Applications, not IdPs, are principally responsible for implementing authorization, while IdPs are principally responsible for implementing authentication. "Authentication strength" is a common authorization consideration.

a. **Role-Based Access Control (RBAC):** Implementation of RBAC to ensure users have appropriate access based on their roles, reinforcing trust and compliance with established policies.

b. **Attribute-Based Access Control (ABAC):** Incorporating ABAC allows for dynamic access control based on user attributes, resource characteristics, and environmental conditions. This flexibility supports a more granular approach to access management, enabling real-time adjustments based on contextual factors.

c. **Zero Trust Principles:** The integration of Zero Trust principles ensures that access is granted based on continuous verification of user identity and context, rather than relying solely on network location or role. This aligns with AAL2 and AAL3 requirements for continuous authentication assurance.

d. **AI-Driven Access Management:** Utilizing artificial intelligence to analyze patterns and behaviors can enhance access control decisions, identifying anomalies and adjusting access permissions dynamically to maintain security.

FEDERATION COMPONENTS

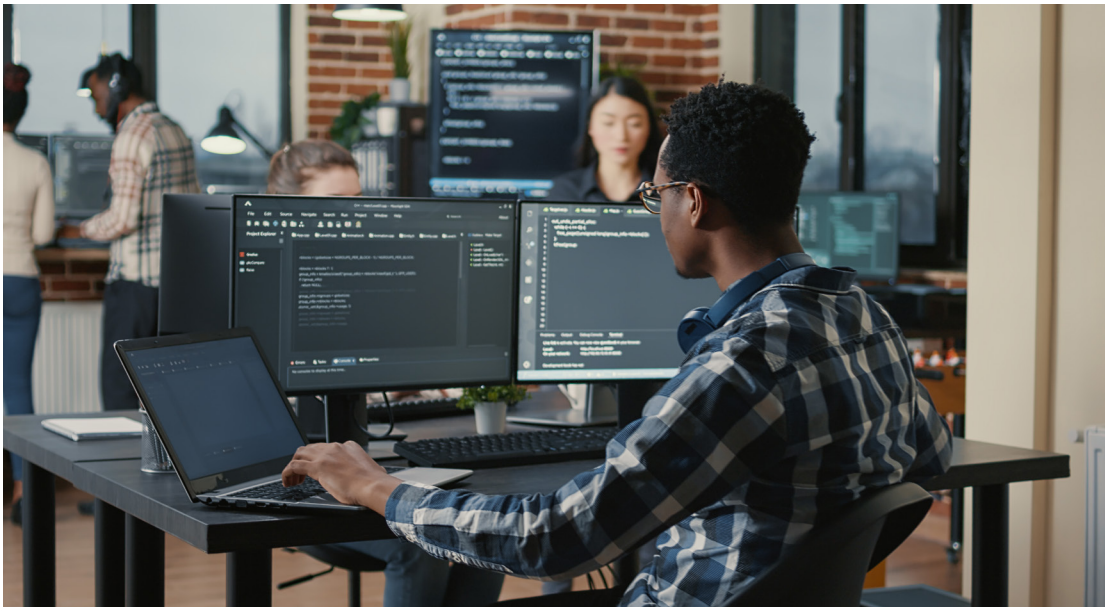
e. **Trust Relationships:** Establishment of mutual trust agreements among agencies to facilitate secure data sharing and access to services, supported by FAL2 or FAL3 federation assurances.

ENTITY METADATA COMPONENT

"Entity" in federations refers to both IdPs and applications (also known as "resource servers" or "protected resources"). within federations typically make metadata available to federation members to promote interoperability and trust. Specific federation agreements must include details about metadata exchange, as well as establishment of shared roots of trust, including specific requirements for entity categories and other access management scoping mechanisms.

Each IdP will register metadata with a Metadata Registration service provided by Technical Managers. IdPs will register the following metadata at a minimum:

- Role Descriptor.
- Entity ID.
- Affiliation Descriptor.
- Contact Person.
- Organization URL.



FEDERATION COMPONENTS

REAUTHENTICATION AND SESSION COMPONENT

Federations may be configured to allow for provisioning on first use. “Reauthentication” refers to subsequent authentication events on behalf of the same user. The application initiates a secure session for the user following validation of the assertion or token provided. The IdP performs authentication ceremonies on behalf of the application and must support session management by the application, including revocation, logout, reauthentication, and timeout.

DoD Framework section: In a federated environment, the RP manages its sessions separately from any sessions at the IdP. T he session at the RP starts when the RP processes the federation protocol from the IdP. At the time of a federated login, the subscriber may have an existing session at the IdP, which may be used as part of the authentication process to the RP. The IdP shall communicate any information it has regarding the time of the latest authentication event at the IdP, and the RP may use this information in determining its access policies. Depending on the capabilities of the federation protocol in use, the IdP should allow the RP to request that the subscriber re-authenticate at the IdP as part of a federation request.

The subscriber is capable of terminating sessions with the IdP and RP independently of one another. The RP will not assume that the subscriber has an active session at the IdP past the establishment of the federated log in. The IdP will not assume that termination of the subscriber’s session at the IdP will propagate to any sessions that subscriber would have at downstream RPs.)

FEDERATION ENTITY IDENTITIES COMPONENT

Federations must define specific requirements for identifying IdPs and resource servers (or applications, relying parties (RP).

A Federation Entity Identity (ID) is a globally unique name for a Federation entity, i.e., your IdP or SP. It is how other services identify your entity. Like any other unique identifiers, you share to interoperate with others, making sure your identifier is clear, unique, and permanent is critical for successful continued operation of your service(s).

Make every effort to choose an ID that will persist indefinitely. Services that interoperate with you, use your ID to look up your metadata. Changing an ID once your service (IdP or SP) is in operation leads to complicated change management efforts across all federation members.

FEDERATION COMPONENTS

Tips for creating a clear, meaningful ID:

- An ID SHOULD be an absolute URL starting with “https://”
- The URL SHOULD NOT contain a port number, a query string, or a fragment identifier
- The host part of the URL SHOULD NOT contain the substring “www”
- The URL SHOULD NOT end with a slash (/)
- An ID SHOULD NOT be more than 30 characters in length
- Include the substring “idp” in an IdP ID
- Include the substring “sp” in an SP ID

Additional notes: An ID is a name. It need not be a resolvable web location. SAML entity IDs must be a Universal Resource Identifier (URI). An ID is a persistent identifier, not a web location. An ID need not resolve to an actual web resource.

REFERENCES & STANDARDS

a. **Legal and Regulatory Frameworks:** Reference relevant laws and government policies on data protection and cybersecurity.

- **Federal Information Security Management Act (FISMA):** The Federal Information Security Management Act (FISMA) is a United States federal law enacted in 2002 (and updated in 2014 as the Federal Information Security Modernization Act) that requires federal agencies to develop, document, and implement information security programs to protect their information and information systems.
    - FISMA's relationship with NIST (National Institute of Standards and Technology) special publications (NIST SPs) is direct and foundational:
    - FISMA specifically authorizes NIST to develop security standards and guidelines for federal information systems (such as Federal Information Processing Standards (FIPS)
- **Federal Information Processing Standard (FIPS)-201:** FIPS-201, also known as Personal Identity Verification (PIV) of Federal Employees and Contractors, is a Federal Information Processing Standard published by the National Institute of Standards and Technology (NIST).

REFERENCES & STANDARDS

Key aspects of FIPS-201:

- Published in response to Homeland Security Presidential Directive 12 (HSPD-12)
- Establishes standards for secure and reliable identification of federal employees and contractors
- Defines a common identification credential for physical and logical access to federal facilities and information systems
- Specifies the architecture and technical requirements for PIV cards
- Includes requirements for identity proofing, registration, and issuance processes
- Incorporates biometric data (fingerprints, photographs) for authentication
- Requires multi-factor authentication through cryptographic mechanisms
- Current version is FIPS-201-3, published in 2022
- **Federal Information Processing Standard (FIPS)-140:** FIPS 140 (Federal Information Processing Standard Publication 140) is a U.S. government standard that specifies security requirements for cryptographic modules used in protecting sensitive but unclassified information.

Key aspects of FIPS 140:

- Developed by NIST in coordination with the Communications Security Establishment Canada (CSEC)
- Current version is FIPS 140-3, adopted in 2019 (replaced FIPS 140-2)
- Defines four security levels, from Level 1 (lowest) to Level 4 (highest)
- Addresses various areas of security including:
- Cryptographic module specification

REFERENCES & STANDARDS

- Cryptographic module ports and interfaces
- Roles, services, and authentication
- Physical security
- Operational environment
- Cryptographic key management
- Self-tests
- Design assurance
- Mitigation of attacks
- FIPS 140 validation is required for cryptographic modules used in federal systems that handle sensitive but unclassified information. Commercial products seeking to sell to federal agencies often pursue FIPS 140 validation through accredited testing laboratories. This standard helps ensure that cryptographic implementations meet minimum security requirements, supporting broader FISMA compliance efforts.

- **NIST SP 800-63:** NIST SP 800-63 is a suite of special publications titled “Digital Identity Guidelines” that provides technical requirements for federal agencies implementing digital identity services.

Key aspects of NIST SP 800-63:

- Current version is NIST SP 800-63-4 (2nd Public Draft), published in August 2024
- Consists of four documents:
- SP 800-63 (Overview document)
- SP 800-63A (Identity Proofing and Enrollment)
- SP 800-63B (Authentication and Lifecycle Management)
- SP 800-63C (Federation and Assertions)
- Introduces three Identity Assurance Levels (IAL) for identity proofing

REFERENCES & STANDARDS

- Defines three Authenticator Assurance Levels (AAL) for authentication strength
- Establishes three Federation Assurance Levels (FAL) for federation security
- NIST SP 800-63 supports FISMA compliance by providing detailed technical guidance for secure digital identity management, which is a critical component of an organization's overall information security program. Federal agencies must align their identity management practices with these guidelines to protect their systems and information effectively.
- **NIST SP 800-217:** Titled "Guidelines for the Use of Attribute-Based Access Control," is a special publication that provides guidance on implementing Attribute-Based Access Control (ABAC) in federal systems.
    - NIST SP 800-217 supports FISMA compliance by helping federal agencies implement more flexible and secure access control mechanisms. ABAC allows for fine-grained access decisions based on multiple factors rather than just roles, which can enhance security while maintaining operational efficiency.
- **NIST SP 800-157r1:** Titled "Guidelines for Derived Personal Identity Verification (PIV) Credentials," provides technical guidelines for implementing derived PIV credentials on mobile devices.
    - NIST SP 800-157 supports FISMA compliance by extending the PIV infrastructure to mobile devices, ensuring that federal employees and contractors can securely access information systems using various devices while maintaining appropriate security controls. This publication helps agencies adapt their identity and access management practices to mobile environments while still meeting federal security requirements.

b. DoD ICAM Federation Framework (https://dodcio.defense.gov/Portals/0/Documents/Cyber/ICAM-FederationFramework.pdf): The Department of Defense (DoD) Identity, Credential, and Access Management (ICAM) Federation Framework is a comprehensive approach to managing digital identities, credentials, and access across the DoD enterprise and with external partners.

REFERENCES & STANDARDS

Key aspects of the DoD ICAM Federation Framework:

- Establishes standards for interoperable identity management across DoD components
- Enables secure information sharing between DoD and external partners (federal agencies, allies, contractors)
- Aligns with the Federal ICAM (FICAM) architecture while addressing DoD-specific security requirements
- Incorporates multiple credential types including Common Access Card (CAC), PKI certificates, and derived credentials
- Implements attribute-based access control (ABAC) for fine-grained authorization decisions
- Supports Zero Trust Architecture principles through continuous authentication and authorization
- Leverages Security Assertion Markup Language (SAML), OpenID Connect, and OAuth 2.0 standards for federation
- Provides mechanisms for cross-domain identity federation with appropriate security controls
- Includes governance structures for managing federated identities and access policies
- The framework helps DoD comply with federal security mandates while enabling mission-critical information sharing across organizational boundaries. It addresses the unique security challenges of military operations while maintaining interoperability with broader federal identity management initiatives.

c. **Best Practices and Standards:** Align with industry standards (e.g., NIST, ISO) for identity management and trust. Existing examples of international trust frameworks include:

- **New Zealand:** The New Zealand Trust Framework, officially known as the Digital Identity Services Trust Framework (DISTF), is New Zealand's approach to creating a secure, interoperable digital identity ecosystem. The Framework supports secure digital transactions while protecting privacy, giving individuals greater control over their identity information, and reducing compliance costs for businesses. It enables reliable identity verification across organizations while maintaining appropriate security controls and privacy protections.

REFERENCES & STANDARDS

- **EU eIDAS:** eIDAS (Electronic IDentification, Authentication and trust Services) is a European Union regulation that establishes a framework for secure electronic identification and trust services across EU member states. eIDAS 2.0, proposed in 2021, aims to expand the regulation to include a European Digital Identity Wallet framework that would provide EU citizens with universal digital identity capabilities for both public and private sector services. While eIDAS is a European initiative, it has global implications for international digital identity standards and interoperability, including potential alignment with US federal identity management frameworks.

- **Pan Canadian Trust Framework (PCTF):** The Pan-Canadian Trust Framework (PCTF) is Canada's approach to creating a national digital identity ecosystem that enables secure and privacy-respecting identity verification across public and private sectors.

Key aspects of the PCTF:

- Developed by the Digital ID & Authentication Council of Canada (DIACC)

- Provides a set of standards, guidelines, and assessment processes for digital identity systems

- Focuses on interoperability between federal, provincial, and territorial identity systems

- Establishes common rules for identity verification, authentication, and federation

- Includes privacy and security requirements based on Canadian legislation and standards

- Features a conformance criteria methodology for assessing compliance

    - Addresses various identity components including:

    - Person/Organization verification

    - Credential issuance and management

    - Authentication

    - Notice and consent

REFERENCES & STANDARDS

- Infrastructure (security and privacy)
- Federation

- The PCTF enables jurisdictions and organizations to issue and accept each other's digital identities through mutual recognition, reducing redundancy in identity verification processes while maintaining high security standards. It aligns with international identity frameworks while addressing Canada's unique federated governance structure and privacy regulations.

- **Others:** Several other significant digital identity trust frameworks exist globally:

  - **Australian Trusted Digital Identity Framework (TDIF) -** Australia's comprehensive approach to digital identity, establishing standards, rules, and accreditation processes for identity service providers across public and private sectors.

  - **Singapore's National Digital Identity (NDI) -** Built around SingPass, providing citizens with secure digital identity for government and private sector services.

  - **India's Aadhaar Ecosystem -** While not traditionally called a trust framework, it establishes comprehensive governance for the world's largest biometric ID system.

  - **UK Digital Identity and Attributes Trust Framework (DIATF) -** Sets rules for organizations providing identity verification services, with a focus on inclusion and privacy.

  - **Nordic-Baltic eID (NOBID) -** A cross-border collaboration enabling mutual recognition of national eID systems across Nordic and Baltic countries.

  - **UAE Pass -** The United Arab Emirates' national digital identity platform and associated trust framework.

  - **Financial Action Task Force (FATF) Digital ID Guidance -** While not a framework itself, it establishes standards for using digital ID in financial services globally.

REFERENCES & STANDARDS

d. GSA Acquisition Vehicles for Credential Service Providers

- https://gsa.federalschedules.com/resources/new-it-sin-for-credential-service-providers/#market
- GSA Special Item Number (SIN) 541519PKI

ATARC