Exchange Network Partnership Grant Project:

E-Enterprise Federated Identity Management (EE-FIM) System

Overview, Partner Integration and Gap Analysis

Document Structure

Document Structure 2

Introduction 6

Partners and Stakeholders 7

Glossary of Terms 7

Project Overview 10

- Project Mission Statement 10
- Project Goals 10
- Implementation Benefits 12
- Project Considerations 13
  - Security-Related Concerns 13
  - Openness, Flexibility and Standards 13
  - Reduced Burden for Partners 13
  - Outreach 13

The E-Enterprise Federated Identity Management System (EE-FIM) 14

- Executive Summary 14
- EE-FIM Trust Framework Structure 15
  - Overview 15
  - Hierarchical Trust Framework and Single Sign-On (SSO) 17
  - Standalone Identity Providers (IdP) 17
  - Relying Party (RP) Extensions 17
- EE-FIM Roles: Identity Providers (IdP) and Relying Parties (RP) 18
  - Identity Provider (IdP) Role 18
    - Level of Assurance (LoA) Summary 18
    - Functional Responsibilities of an Identity Provider (IdP) within the EE-FIM System 19
    - Pros and Cons of Being an Identity Provider (IdP) 19
      - Pros 19
      - Cons 20
  - Relying Party (RP) Role 20
    - Functional Responsibilities of a Relying Party (RP) 21
    - Pros and Cons of being a Relying Party (RP) 21
      - Pros: 21
      - Cons: 21

Shared CROMERR Services (SCS) Integration with the E-Enterprise Federated Identity Management (EE-FIM) System **23**
The Concept of Integrating SCS with EE-FIM 23
The SCS + EE-FIM User Story: 23
SCS as Dependent Services to a Relying Party 24
Determination and Definition of Dependent Service Role 24
How the SCS Works As a Dependent Service Under EE-FIM 25
SCS References 26
The Benefits of Integrating SCS with EE-FIM 28
EE-FIM Facilitates Access to Shared CROMERR Services 28
Addressing Partner Perspectives and Concerns with SCS and EE-FIM 28
North Dakota 28
Wyoming 29
Agreed-Upon Next Steps 29

Recommendations & Continued Work **32**
EE-FIM & SCS Integration, Recommendations & Next Steps 32
Identity Provider (IdP) Recommendations & Next Steps 32
Relying Party (RP) Recommendations & Next Steps 32
EN Enterprise Security Bridge Recommendations & Next Steps 33
Governance Recommendations 34
Operations and Support Procedures 34
Standards and Policies 35
Research and Development 36

Summary **36**

Appendix A: Technical Details **40**
The EPA Enterprise Security Bridge 40
The EN Enterprise Security Bridge's Multi-Protocol IdP Manager 42
Technical Details of IdP and RP Roles 43
IdP Authentication Details 43
IdP and Secure Tokens - Behind the Scenes 44
RP Validation Details 44
RP Claims Processing 45
Traversal and Single Sign-On (SSO) 45
Additional benefits of passive validation in a federated SSO system: 45
Supplementary Project Documentation 46

Appendix B - Integration Options for IdP and RP Roles **47**
Identity Provider (IdP) Options 47

Guidance for Partners - Identity Provider (IdP) 47
Declined Identity Provider (IdP) Options 48
Relying Party (RP) Options 48
Guidance for Partners - Relying Party (RP) 49
Declined Relying Party (RP) Options 49

Appendix C - Partner Integration Engagements 51
Partner Discovery Sessions 51
New Mexico Environment Department 52
New Mexico Discovery and Analysis 52
NMED Technology Platform 52
NMED Single Sign-on System 52
NMED Discovery Session 53
Identified Strengths of the SEP IDM: 53
Identified Weaknesses of the SEP system: 53
New Mexico Integration Solution 55
Integration Choices 56
Identity Provider (IdP) Integration 56
IdP Integration Difficulty Level and Implementation Time 56
Relying Party (RP) Integration 57
RP Integration Difficulty Level and Implementation Time 57
Identity Provider and Relying Party Integration Steps 57
Recommended tools, frameworks, web resources 58
Wyoming Department of Environmental Quality 59
Wyoming Discovery and Analysis 59
WDEQ Technology Platform 59
WDEQ Identity Management System (IDM) 59
WDEQ Discovery Session 60
Identified Strengths of current eGov / ENVITE IDM system: 60
Identified Weaknesses of the eGov / ENVITE IDM system: 60
Wyoming Integration Solution 63
Integration Choices 63
Identity Provider (IdP) Integration 63
IdP Integration Difficulty Level and Implementation Time 64
Relying Party (RP) Integration 64
RP Integration Difficulty Level and Implementation Time 64
Identity Provider and Relying Party Integration Steps 64
Recommended tools, frameworks, web resources 65
North Dakota Department of Health 66

North Dakota Discovery and Analysis 66
NDDOH Technology Platform 66
NDDoH Identity Management System (IDM) 66
NDDoH Discovery Session 67
Identified Strengths of current NDDoH IDM system: 67
Identified Weaknesses of the NDDoH IDM system: 67
North Dakota Integration Solution 70
Identity Provider (IdP) Integration 71
IdP Integration Difficulty Level and Implementation Time 71
Relying Party (RP) Integration 71
RP Integration Difficulty Level and Implementation Time 72
Identity Provider and Relying Party Integration Steps 72
Recommended tools, frameworks, web resources 72

Appendix D - Traversal Whitepaper sent to EPA OEI on 2/12/17 73

Appendix E - Recommendations Document sent to E-Enterprise Management Board on July 14, 2017 82
Background 82
Identity Provider (IdP) Recommendations 84
Relying Party (RP) Recommendations 85
Identity Bridge Recommendations 86
EPA Identity Bridge – Proposal for Federated Single Sign On 86
Governance Recommendations: 87

E-Enterprise Federated Identity Management (EE-FIM) System

Introduction

The US EPA and Office of Environmental Information (OEI) recognised several years ago the need for what has come to be known as the Federated Identity Management System. This system was envisioned to be a means for disparate entities to accept the authentication of one another's users as though they had logged on directly to their own system. At the same time as providing ease of access, it would still ensure a Level of Assurance that allowed authorization to a given application.

Described in this document are the results of a collaborative project between three states and the EPA. Led by New Mexico, a working proof-of-concept of a trusted framework has been implemented that allows users to securely traverse between state systems and the E-Enterprise Portal without the need to re-authenticate to each individual system. This provides all network partners with a seamless and efficient user experience to customers that do business with various environmental agencies.

This document specifically describes the steps and effort taken to conceive and create this trusted framework. Known as the E-Enterprise Federated Identity Management (EE-FIM) System proof-of-concept, the particulars of how this integrated system is fully realized are described in detail.

Also documented are the current technical platform, identity management program, implementation choices, integration steps and gap analysis for each partner within this collaboration. Proposed improvements to the system to reduce the burden for participation, enhance the user experience and enhance security across multiple states and agencies are addressed. Furthermore, the results of the research and discussion with project partners regarding the possible use cases and means of integration of EPA Shared CROMERR (Cross-Media Electronic Reporting Rule) Services with EE-FIM are included.

Partners and Stakeholders

The following agencies and departments actively participated in the project and without their invaluable support and knowledge, this project would never have been successful:

- U.S. Environmental Protection Agency (EPA) - Office of Environmental Information (OEI)
- Wyoming Department of Environmental Quality (WDEQ)
- North Dakota Department of Health (ND DoH)
- New Mexico Environment Department (NMED)

Glossary of Terms

In order to fully comprehend this document's contents, various terms and acronyms used throughout are listed here for reference:

AES - *Advanced Encryption Standard* is a *NIST* security standard commonly used for secure electronic communications, such as the web's HTTPS secure protocol

Authentication - An operation to ensure a subject's identity is genuine as claimed. The subject must present a proof of identity (credential) in order to be successfully authenticated

Authorization - An operation to give a subject permission to perform a certain task

COTS - Commercial Off The Shelf software

Cross Media Electronic Reporting Rule (CROMERR) - Provides the legal framework for electronic reporting under EPA's regulatory programs. The Rule sets performance-based, technology-neutral system standards and provides a streamlined, uniform process for Agency review and approval of electronic reporting. The CROMERR program ensures the enforceability of regulatory information collected electronically by EPA and EPA's state, tribal and local government partners

Federated Identity Management (FIDM) - The means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems

E-Enterprise Federated Identity Management System (EE-FIM) - End-product developed by the collaborative project between EPA, NMED, WDEQ and ND DoH

ENV-ITE - The Environmental IT Environmental System is the single sign-on application used by WDEQ for statewide access to their applications

ERIS - The Electronic Reporting Information System is the Identity Management System used by the North Dakota Department of Health

EN Enterprise Security Bridge - Centralized Authentication Engine developed by EPA OEI to enable authentication options for users

Identity Management System (IDM) - An information system or set of technologies that can be used for enterprise or cross-network management of user identities

Identity Provider (IdP) - *Is a service that* authenticates users by means of security tokens and provides assertions about the user attributes to the clients of the service (Relying Parties)

NIST - The National Institute of Standards and Technology promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology

OpenID - An open standard and decentralized authentication protocol

OIDC - Open ID connect; A simple identity layer built on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner

OSOTS - Open Source Off the Shelf software

PHP - Hypertext Preprocessor is a server-side scripting language designed for Web development

Relying Party (RP) - An application/system that depends on security services from a third party

Representational State Transfer (REST) - An architectural style for web services based on HTTP that allows access to web resources via a set of stateless operations

Secure Extranet Portal (SEP) - NMED's single sign-on system

Secure Token Services (STS) - Software based identity provider responsible for issuing security tokens, especially software tokens, as part of a claims-based identity system

Security Assertion Markup Language (SAML) - An XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider

Separation of Concerns - A design principle under which a software application is parceled into distinct sections, such that each section addresses a separate concern or set of information that affects the operation of the application.

Shared CROMERR Services (SCS) - Services offered by the EPA that can be leveraged to achieve CROMERR compliance

Simple Object Access Protocol (SOAP) - a messaging protocol specification based on XML for exchanging structured information in the implementation of web services

Single Sign On (SSO) - With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames/passwords

Additional IDM Terminology can be found here: IDM Terms List

Project Overview

The E-Enterprise (EE) Shared Identity Management Concept of Operations (June, 2015) provided the original blueprint for a seamless experience for users traversing between partner applications and the EE Portal. Section 4.5.1.3 (*E-Enterprise Identity Management*) of that document describes the fundamental components required for the federated identity system specifically describing the EPA-developed Enterprise Security Bridge. This project explores the necessary steps performed by three partner states to integrate their existing identity management systems and web applications with the Enterprise Security Bridge, the centralized hub identified in that section of the document.

The New Mexico Environment Department (NMED) worked with partner states Wyoming (WY DEQ) and North Dakota (ND DOH), as well as with EPA Office of Environmental Information (OEI) staff from the E-Enterprise Portal and the Enterprise Security Bridge teams to implement a working proof of concept to verify the technical feasibility of establishing a federated identity management system for co-regulator partners - one where a user could log in with their local system credentials (IdP role) and access web resources (RP role) within the trust network. Once the proof-of-concept of this system was in place it demonstrated how users could effortlessly travel between the partner web applications managed by those identity systems and the E-Enterprise Portal.

Project Mission Statement

“The mission of the E-Enterprise Identity Solution Project is to test the process of integrating three very different State systems with the existing EN Enterprise Security Bridge, which was developed to provide a federated identity management system for EPA systems and the E-Enterprise Portal.

Through the experience of this integration work, the team will identify opportunities for improvement of the current system. Recommended improvements should meet the following criteria:

- reduce burden to the partners,
- enhance the user experience,
- increase adoption among partners and
- ensure safe and secure interactions within the system.”

Project Goals

The straightforward goal of the project is to identify best how to authenticate users a single time and allow secure access to other related sites without the user having to re-authenticate as illustrated in *Figure 1* below. .

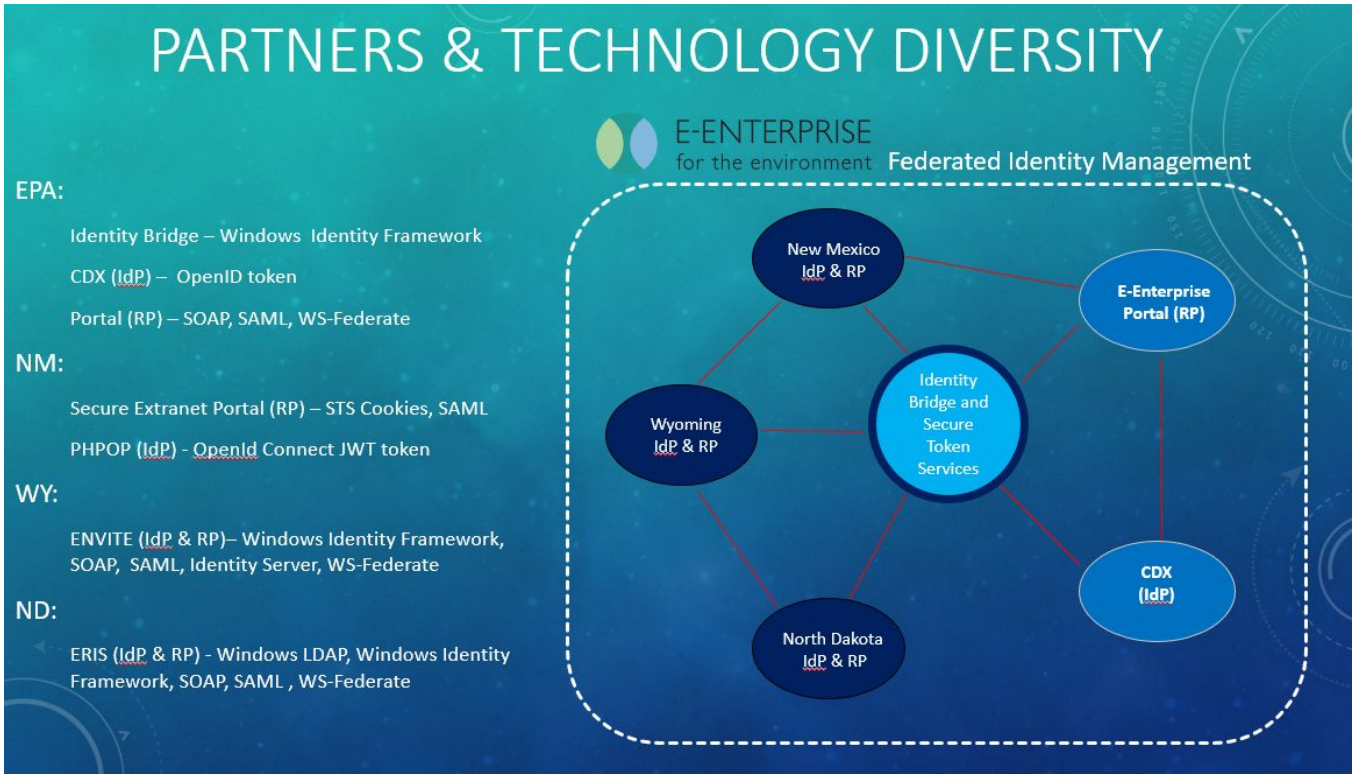


Figure 1: Proof-of-concept Partners Technology Diversity

If successful, this E-Enterprise Identity Management (EE-FIM) system could facilitate transacting business among co-regulators and between the regulated community and co-regulators. Expanding adoption to additional partner systems will be the next focus for increasing the business value that could be realized with more systems participating in the system as *Figure 2* illustrates.

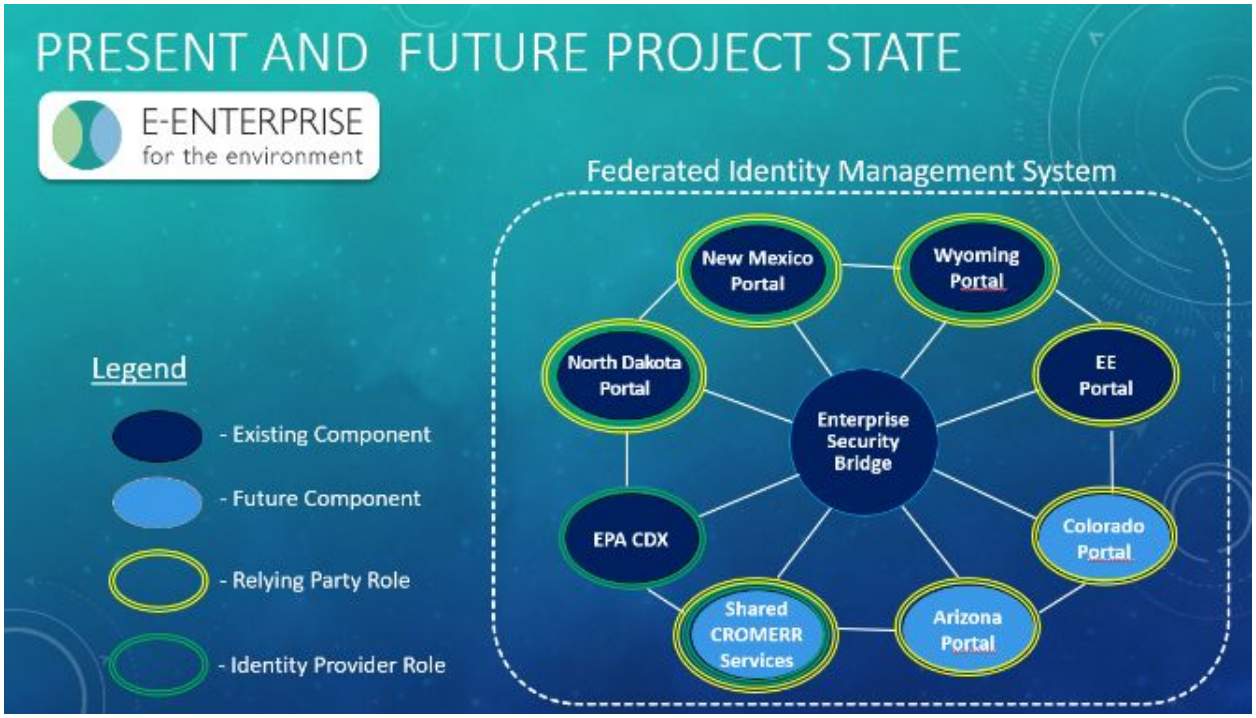


Figure 2: Future partner target

Implementation Benefits

A component of the project involved identifying the benefits of implementing such a solution. That analysis revealed that the EE-FIM system allows quite a few benefits to be realized including the following:

- Increased user privacy and security of user credentials - Maintaining a single set of credentials minimizes the chance of incorrect, out-dated or inconsistent user information and facilitates a single source of change if a breach occurs.
- Reduced cost and burden associated with registering and maintaining multiple identities across applications - User registration takes time and often involves support from system staff. A streamlined implementation reduces the overhead associated with the process.
- Increased accuracy and currency of user information (claims) - Consolidated information within a single set of credentials can contain more information that would likely be maintained by individual sites and since the account is frequently used it's more likely to be kept up-to-date.
- Enhanced user experience (fewer passwords and seamless traversal) - A single login ID and password is simply easier to keep track of reducing the confusion among sites and the need to contact support staff for help.
- Promotes collaborative work between co-regulators and the regulated community to provide more timely and accurate data across the Enterprise - If users have the ability to

use their credentials to traverse to a partner site or application they are more likely to take advantage of the functionality that it can offer.
- Positively impacts potentially hundreds of co-regulators and tens of thousands of regulated entities - It reduces the labor necessary in order to comply with reporting regulations.
- Provides a means by which co-regulators could implement improved environmental management workflows, by eliminating barriers between agencies and entities - Simply the act of having co-regulators cooperate often presents the opportunity for them to explore what each partner can offer ultimately leading to better tool and data availability.
- Provides Single-Sign-On functionality to entities that lack the resources to create such a system for themselves - various states do not have the resources to build their own single sign-on functionality and making it readily available would allow them to adopt it.

Project Considerations

In a project of this nature there are a number of topics that warrant careful consideration. Each of the following were taken into account while crafting the approach that was used to implement the proof-of concept solution:

Security-Related Concerns

Security needs to be at the forefront of any distributed implementation and so the trust and Level of Assurance between Identity Providers and Relying Parties must be a focus point of the solution and actively considered throughout the process.

Openness, Flexibility and Standards

The rapidly evolving Internet of Things makes an important consideration the need to adopt modern, yet widely-used standards while supporting decentralized authentication protocols. It is important to evaluate the various technological options available and choose a direction that is easily adaptable and will be used for the foreseeable future.

Reduced Burden for Partners

The success of any project often lies within how easily it can be adopted and integrated by anyone who tries to incorporate its functionality. To this end, a big consideration for this project is to provide an end-product that is straightforward to integrate, implement and maintain. Providing the best end-user experience is a key consideration.

Outreach

Related to reducing the burden to partners for an effort such as this is providing great communication, documentation and tools to be able to successfully integrate the solution. There

are both technical and non-technical hurdles associated with integrating into this system and so another main consideration is how product outreach is handled.

The E-Enterprise Federated Identity Management System (EE-FIM)

Executive Summary

The E-Enterprise Federated Identity Management System (EE-FIM) is comprised of the Enterprise Security Bridge as a centralized broker within the system, partner Relying Parties, partner Identity Providers and Dependent Services to Relying Parties. This project's focus centered on integrating as trusted web entities, three state systems (New Mexico, North Dakota and Wyoming) with the Bridge; providing traversal access to the previously integrated EPA E-Enterprise Portal. Additionally, planning and design work with the EPA Shared CROMERR Services team provided a useful path forward for incorporating Shared CROMERR Services as Dependent Services to a Relying Party.

As depicted in *Figure 3* below, the EN Enterprise Security Bridge acts a centralized broker within the system. It translates secure tokens from registered Identity Providers (IdP) to a standard security token for use within the EE-FIM network. The Security Bridge also validates the security tokens for registered Relying Parties (RP). Partner portals and web applications can perform the role of a Relying Party (a service provider to trusted entities), an Identity Provider (identity store and credential issuer) or both.

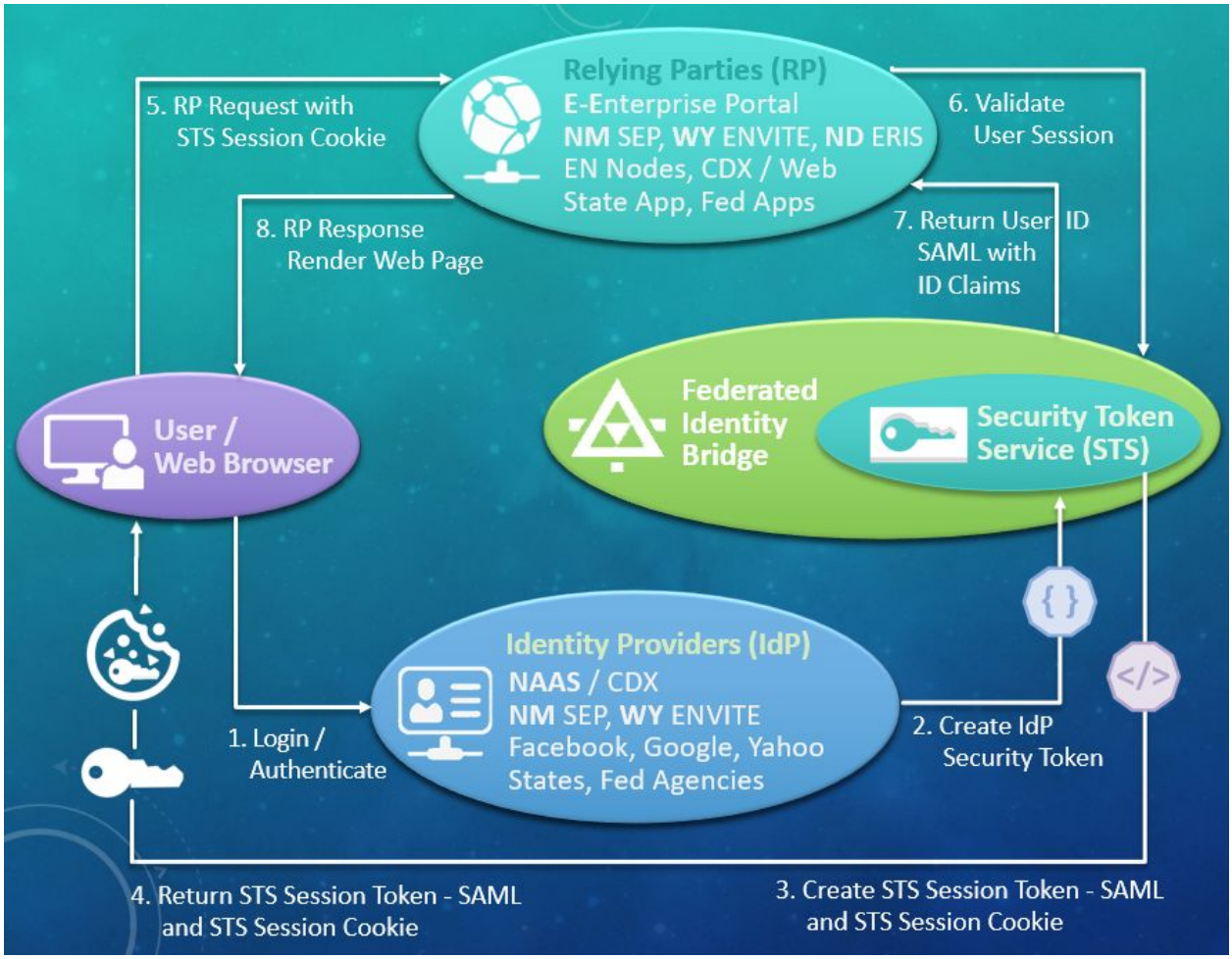


Figure 3: EE-FIM System Diagram

EE-FIM Trust Framework Structure

Overview

The EE-FIM structure diagram (*Figure 4*, below), depicts the structure of the EE-FIM including its primary components and the relationships between them. Taken together, the connections illustrated by the bold yellow lines (both solid and dashed lines) and the connected entities, represent the EE-FIM trust framework or ecosystem. The state and federal partners establish trust with the EN Enterprise Security Bridge via registration and an exchange of keys. They also create trust through governance and policy agreements to participate in the EE-FIM. For example, when a Wyoming ENVITE account holder logs in via the ENVITE identity provider (IdP), EE-FIM relying parties (RPs) -- such as New Mexico's SEP gateway and North Dakota's ERIS web application -- trust that the Wyoming user has a valid account. Further, they trust that the Bridge has checked the registered key of the Wyoming ENVITE IdP, and that the IdP has checked the registered key of the Bridge (see dashed yellow lines). Finally, they trust that the

Bridge's Multi-Protocol IdP Manager converts ENVITE's IdP token and user identity claims into the EE-FIM standardized Security Token and claims, which is a SAML security assertion (see central dotted yellow line).

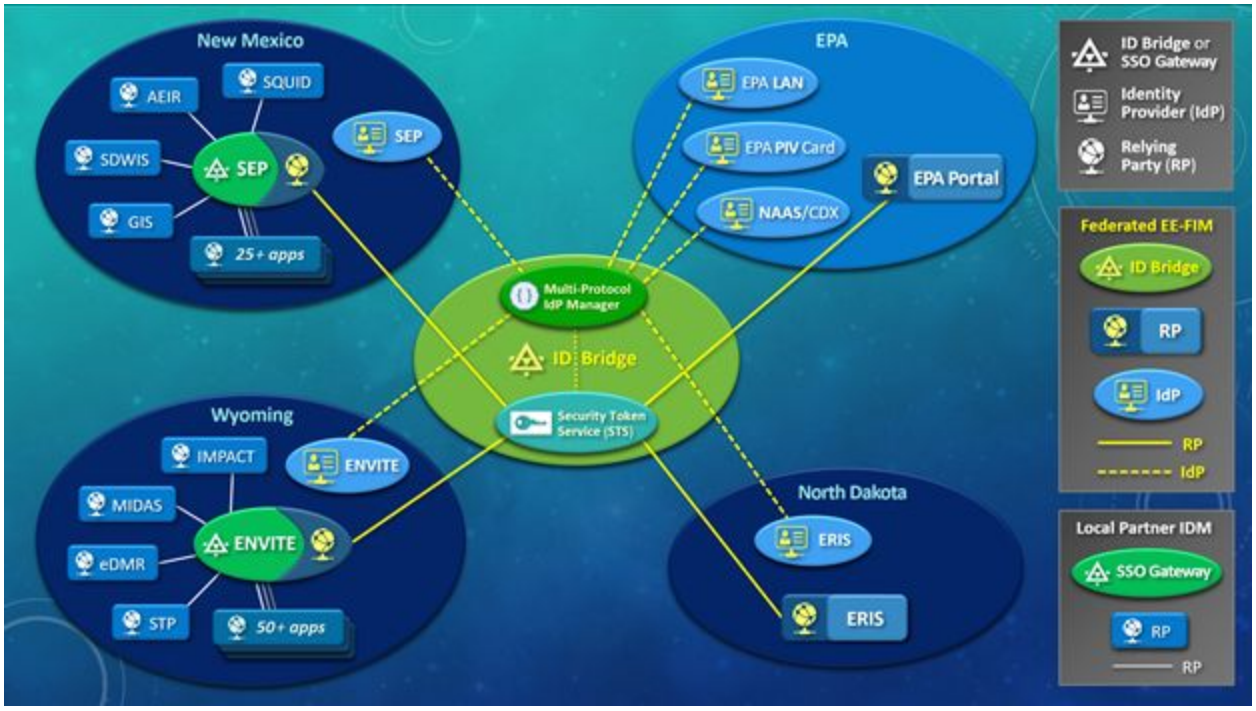


Figure 4: EE-FIM Structure Diagram

Thus, when the Wyoming user arrives at New Mexico's SEP gateway or North Dakota's ERIS web application, SEP or ERIS – acting as an EE-FIM relying party (RP) – will request that the EN Enterprise Security Bridge validate the SAML token accompanying the Wyoming user (see yellow lines connecting RPs to the Bridge's Security Token Service (STS) component). After validating the SAML token, the Bridge then posts the Wyoming user's identity claims back to the relying party (RP). It is then up to the RP to manage the authorization and access of the Wyoming user that was just validated by the Bridge. For instance, New Mexico's SEP (after requiring one-time registration information from the user) will automatically create a SEP account for the external EE-FIM Wyoming user. However, the Wyoming user must also request access to SEP-managed web applications, just as any local New Mexico user must do. The owner of the SEP-managed web application for which the user is requesting access may require additional information from the user in order to make authorization decision concerning the user's request for access. If the Wyoming user has previously done this and been granted access, then the Wyoming user will be routed by SEP to the requested web application resource.

Hierarchical Trust Framework and Single Sign-On (SSO)

A serendipitous result of the EE-FIM structure is that existing Single Sign-On (SSO) gateways, such as New Mexico's SEP and Wyoming's ENVITE, are naturally extended to the federated SSO provided by the EN Enterprise Security Bridge's Security Token Service (STS). This was accomplished by modifying the SEP and ENVITE gateways to be relying parties (RP) of the EE-FIM trust framework. These local SSO gateways can now accept an external user validated by the Bridge's Secure Token Service (STS) – such as the Wyoming user in the above example – possessing a valid Security Token. Continuing with this example, after SEP validates this user via the Bridge's STS, it then issues a local SEP security token just as it would for a local New Mexico user.

This hierarchal SSO behavior is significant because it demonstrates that a natural *conversion* of the security token takes place from the federated EE-FIM trust framework's Security Token (SAML) to the local SSO gateway's security token. In the case of New Mexico's SEP, the local SSO gateway security token is a Java Spring Security JSessionID. Though this behavior functions like a conversion of the token, it is more accurate to say that a second local SSO token is issued in addition to the federated SSO token.

The functional benefit of this capability is that the Wyoming user – continuing our example – may, upon locally approved authorization, visit any of the 30+ web applications managed by New Mexico's SEP gateway without needing any additional login beyond the initial login via the ENVITE IdP on the federated EE-FIM trust framework. More broadly, EE-FIM users may traverse the entire EE-FIM network from state to state, as well as web application to web application *within* a state's network that is managed by a gateway SSO.

More information on the Trust Framework can be found in the Identity Federation and Trust Framework Specifications document. Also additional technical details for the Security Bridge can be found in *Appendix A*.

Standalone Identity Providers (IdP)

The EE-FIM structure diagram (*Figure 4*), reflects the reality that the identity providers (IdP) in the trust framework are standalone server applications. These identity providers are often Commercial Off The Shelf (COTS), Open Source Off The Shelf (OSOTS) software products that are simply installed, configured, and registered with the EN Enterprise Security Bridge. The primary configuration required after installing the IdP is to connect the IdP to the identity store of the state partner's identity management system (IDM).

Relying Party (RP) Extensions

In contrast to the identity providers (IdP) discussed above, the relying parties (RP) in the EE-FIM trust framework are ***not*** standalone software packages. Rather, the relying parties are

existing custom software products that are then *modified* and *extended* to participate as an RP in the EE-FIM trust framework. This is represented in the EE-FIM structure diagram (*Figure 4*) by showing the yellow network globe icon (RP icon) grafted onto existing web applications, such as North Dakota's ERIS, as well as grafted onto existing SSO gateways, including New Mexico's SEP and Wyoming's ENVITE. The software modifications required to participate as an EE-FIM Relying Party are: connection to the EN Enterprise Security Bridge via the WS-Federation protocol, token validation via HTTPS redirect to the Bridge (or via SOAP web service calls to the Bridge), decoding and parsing SAML assertions to obtain the user's identity claims, connecting the EE-FIM claims to the RP's local IDM, and in the case of gateway SSO systems, verifying the user within the local system and optionally, issuing a local security token.

EE-FIM Roles: Identity Providers (IdP) and Relying Parties (RP)

Each of the EE-FIM partners (states, tribes, municipalities, federal agencies, web applications, etc.) may participate in the EE-FIM ecosystem in either or both of the Federated Identity Management Roles: *Identity Provider (IdP)* and *Relying Party (RP)* - see *Figure 4*, above.

Identity Provider (IdP) Role

Identity Providers (IdPs) supply authentication (login) services by means of security tokens and and provides assertions about the user claims to the entities using the service (Relying Parties). IdPs may support various levels of rigor in confirming a given user's identity. This Level of Assurance (LoA) identity proofing ranges from low-trust (e.g. *Login with Facebook*) to high-trust (e.g. Top-Secret federal credential - verified by driver's license, social security card, birth certificate, and background investigation). The LoA also depends on the technical security of the authentication (login) process, ranging from simple password to multi-factor authentication with a hardware cryptographic token (e.g. PIV card) or biometric (e.g. fingerprint) factor.

Level of Assurance (LoA) Summary

While some work remains to be done regarding the determination of Levels of Assurance in the EE-FIM system (see *Appendix E*), below is a brief summary of the NIST standard requirements for LoA, which might serve as a point of departure for EE-FIM specific LoAs. (see https://www.nist.gov/ for more detailed information)

Level 1 – No identity proofing. Authentication by password via basic web encryption.

Level 2 – Identity proofing via primary government photo ID, name, date of birth, and address or phone number. Authentication by single factor - strong password or higher method. Secure authentication preventing eavesdropper, replay, and guessing attacks.

Level 3 – Identity proofing requires verification of identifying materials and info (see LoA 2). Authentication requires proof of possession of a cryptographic key with either a "soft" token (typically apps that run on phones or laptops) or a "hard" token (provided by a hardware

device). The authentication mechanism must prevent token compromise by eavesdropper, replay, guessing, verifier impersonation, and man-in-the-middle attacks. Also requires two factor authentication: key plus password or biometric to activate the key.

Level 4 – Applicant must appear in-person before registration officer. Verification of two independent ID documents or accounts is required including a primary government photo ID. Also, a biometric recording of the applicant at the time of application is required. Authentication requires two factor authentication including proof of possession of a “hard” cryptographic token. Additionally, subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security.

Functional Responsibilities of an Identity Provider (IdP) within the EE-FIM System

An Identity Provider (IdP) must deploy a web service that implements the functions and protocols of an IdP. This is not typically a big lift when using standard free IdP software which provides these services. The functional responsibilities of the IdP role include:

- Providing a publically available server that is well-secured (e.g. firewall and whitelist) and which has high availability (e.g. 99%+ “up” time).
- Choosing and installing an IdP web service appropriate for the technology stack.
- Being responsible for identity proofing registered users, maintaining their data in the local Identity Store, and determining the LoA for these users.
- Configuring the IdP to connect to the local Identity Store. The configuration options include protocol connection (e.g. Active Directory or LDAP), database connection, and web service connection.
- Registering the IdP with the EN Enterprise Security Bridge, which includes an exchange of keys.
- Gathering user information from the local Identity Store to submit as claims and formatting them into a Bridge-supported IdP token (e.g. JWT, SAML).

Pros and Cons of Being an Identity Provider (IdP)

Pros

- A Partner’s existing user-base can use a credential they already have (e.g. NM SEP, WY ENVITE). Note: this is known as a Bring Your Own Credential (BYOC) system - there is a very popular example in the education sector, called Shibboleth, where thousands of graduate research institutions all participate in a FIM using BYOC with their own university’s login account credentials.
- An EE-FIM Partner can control their own identity proofing standards - e.g. notarized signature, proof of employment with a facility, driver’s license, social security card, birth certificate, or combinations of these. This, in turn, allows control over the LoA standard - see above subsection LoA Summary defining these standards.

- High-quality free (open source) and commercial software products are available for all popular platforms - Linux/Apache/(Java EE or PHP), Windows/IIS/.NET, Windows/Apache/PHP, Mac OS/Apache/(Java EE or PHP)
- As an Identity Provider, the IdP may provide services for additional web applications or trust frameworks - not just EE-FIM. For instance, the IdP could be used by other web applications in the state.
- More control over the infrastructure - for example, any IdP downtime is within the partner's scope to address, rather than having to wait for others.
- Implementing an IdP is a best practice from a software architecture point of view, addressing both "separation of concerns" and complying with "microservices" architecture principles.

Cons

- Unneeded extra work and cost if IdP already provided by others, including liabilities for ongoing maintenance, governance, and even legal work (e.g. contractual identity proofing). For example, the EPA has already deployed an IdP for NAAS/CDX account holders. If your user-base already has such credentials in common, there may be no need for your state to provide their own IdP.
- Standing up an IdP requires time from a system administrator or software engineer to install and configure. Allow time for testing and maintenance as well.
- If users outside your state utilize your IdP services you may encounter additional costs to support these users and scale appropriately.

Relying Party (RP) Role

Relying Parties (RPs) are service providers to trusted entities within the EE-FIM trusted framework. RPs are typically web applications (e.g. ND ERIS), web application gateways (e.g. NM SEP and WY ENVITE), or web services. Because the EN Enterprise Security Bridge provides overall security by allowing only trusted partners to connect, each of the EE-FIM partners can literally *rely* upon the Bridge to allow access *only* to persons who have logged into the EE-FIM via an IdP that is also a trusted partner of the EE-FIM trusted framework. For example, North Dakota's ERIS application integrates with the EE-FIM as a Relying Party (RP). Thus, it relies upon the Bridge to broker an IdP login via, for example, New Mexico's SEP Identity Provider (IdP). A key responsibility for each RP is to ensure appropriate access and authorization based upon the IdP and/or permissions for individual users (accounts). Authorization defines the policy for a user or group of users regarding their access permissions to applications (e.g. view, add, edit, sign, delete, etc.). In many cases, partner RPs will authorize other state partners for read-only access. Additionally, RPs should restrict authorization via social media IdPs (e.g. *Login with Facebook*) that have a low-trust Level of Assurance (LoA). For instance, users logged in with Facebook should be only be authorized to view public facing websites.

Functional Responsibilities of a Relying Party (RP)

A Relying Party (RP) must modify an existing web application or gateway to comply with the protocols, SOAP web service calls and/or redirect endpoints of the EN Enterprise Security Bridge. Additionally, an RP must extend the capabilities of its identity management system to accommodate federated users who have logged in through an IdP via the Bridge. This includes handling the RP aspects of federated single sign-on (SSO). For a Relying Party that is a web gateway (i.e, one with their own Single-Sign-On solution), further modifications are needed to coordinate with the local SSO, as well linking the federated identity to the local identity store. The functional responsibilities of the RP role include:

- Registering your RP with the Bridge, which includes an exchange of keys and endpoint urls.
- Connecting to the Bridge via the WS-Federation protocol.
- Validating the Bridge's federated STS tokens via the Bridge's validate SOAP web service or the Bridge's redirect endpoint for validation.
- Decrypting, verifying, decoding and parsing the SAML assertion returned by the Bridge, which contain the user's Identity Claims.
- Processing the identity claims to extract: userid (email), first name, last name, etc.
- Setting up the appropriate policies for access and authorization, which includes appropriate handling of EE-FIM specific Claims, such as "CROMERR Compliance".
- For gateway RPs, issuing local SSO tokens for federated users.
- For gateway RPs, performing local SSO redirects (based on the URL being accessed by the federated user) to the requested RP-hosted application.
- For gateway RPs, linking the federated identity claims to the local identity store.

Pros and Cons of being a Relying Party (RP)

Pros:

- Extends access of partner's web applications to other trust framework partners.
- Facilitates collaboration and information sharing among state and federal partners.
- Provides timely access to the latest data for trusted partners.
- Provides services onto federated single sign-on (SSO) system. This would allow, for instance, a regulated entity to login in only once and submit data to multiple states.
- Provides single sign on access to web applications for partners without a gateway.
- Ease of implementation - for web applications without a similar identity management mechanism, they can take advantage of one that already exists reducing cost, maintenance and responsibility.

Cons:

- Requires more initial investment of software engineering resources to address the more complex technical integration. Ongoing maintenance and support is also required.

- Entails cooperation and governance to ensure appropriate levels of access to information for state and federal partners.
- EE-FIM Partners without an SSO gateway must modify each of their web applications to implement required RP extensions and register each one with the Bridge.
- Reliance on the Bridge and its IdPs for availability - if those services are down users won't be able to get into their applications and it's out of your own control to address the problems. *Note:* This issue can be greatly mitigated for existing web applications and gateways by implementing your RP to continue to allow users to optionally login via the local IDM system and identity store. This was done by all EE-FIM state partners. For additional information on the technical details for the IdP and RP roles, see *Appendix B*.

Shared CROMERR Services (SCS) Integration with the E-Enterprise Federated Identity Management (EE-FIM) System

The Concept of Integrating SCS with EE-FIM

It was determined early in the project proposal that a Federated Identity Management System and Shared CROMERR Services had the potential for synergetic interactions, and this integration was specified as a project deliverable. It was not initially clear what shape such an integration would take. The project team started out by reaching out to interview the project partners on the topic, along with Alabama Department of Environmental Management, who has concluded a successful direct implementation of SCS on their own. Based on the results of the questionnaires, a clear picture of which aspects of SCS were most desirable from the State perspective was resolved, along with some understanding of the concerns held by the states regarding details of SCS operation, such as Copy-of-Record ownership along with several others.

Armed with this new understanding, the team set about constructing a series of User Stories around use cases of SCS / EE-FIM integration. Eventually by working our way through these stories as thought experiments, the team narrowed down several potential SCS+EE-FIM User Stories into a single, representative User Story that everyone felt encapsulated the critical issues of integration. This reduction was necessary to move forward as the multiple scenarios, all of which were some variation of the representative story, were overwhelming and induced confusion. This single, representative user story was then used as the point of departure for subsequent conversations with the project partners and the EPA SCS Team regarding the exact nature of SCS integration with the Federated trust network.

The SCS + EE-FIM User Story:

A user from the regulated community authenticates onto the EE-FIM network with New Mexico's Secure Extranet Portal (SEP). As part of the business that user is conducting, she then wants to report emissions to a regulatory entity that is a Relying Party on the EE-FIM network. (This RP could also be part of the State of New Mexico, or it could be another RP from another state or public entity that has a trust relationship established with the SEP IdP via the EE-FIM network.)

Once completed, the user certifies the reported emissions and saves the signed emissions report as a Copy of Record. In the background the Relying Party web application to which they're submitting invokes the specific SCS services needed such as the Signature Ceremony +

Copy of Record service[1] - depending on the SCS services the emissions reporting application has implemented. The user experience is unaware of the underlying calls to the SCS services.

After the SCS is invoked, the result is returned to the RP application, which displays a message in accordance with the result retrieved.

While this scenario is relatively straightforward, it actually generated many specific, detail-oriented questions about how SCS could be engaged via the EE-FIM and how exactly the SCS would be integrated with the RP and IdP involved in user authentication and authorization. Those questions resulted in the development by the team of three scenarios in which SCS could be integrated onto EE-FIM; As a traditional Relying Party, as a "Headless" RP, or as a new EE-FIM concept, that of a Dependent Service to a Relying Party. All of these methods had positive and negative aspects, and it was difficult for the team to make a determination as to which approach would be optimal.
As such, the team requested the help of the EPA SCS Team, holding several conference calls and culminating in a two-day, in-person meeting in August 2018 with the SCS Team. Through these efforts the team was able to determine what SCS looks like in the context of EE-FIM, and to outline that sufficiently to provide an implementation path and to have a good idea of what benefits might be derived.

As a result, the team was able to derive a concept of how SCS functions within the context of the EE-FIM system, and this concept evolved into essentially what would be thought of as a third role on the EE-FIM network, alongside those of RP and IdP. This third role can most easily be thought of as Dependent Services to a Relying Party.

SCS as Dependent Services to a Relying Party

Determination and Definition of Dependent Service Role

The question of how SCS would operate within the context of the EE-FIM did not initially possess a clear answer. SCS are web services built around a SOAP (Simple Object Access Protocol) architecture, whereas the EE-FIM, based on the trusted and secure nature of the network, facilitates a REST (REpresentational State Transfer) approach. These two configurations to web services are not typically compatible. It took considerable pondering on the part of the project team, culminating during the in-person meeting with the EPA's SCS team, to answer how this integration could and should take place. As mentioned above, the conclusion arrived at by the participants in this productive two-day session was that SCS should integrate into the EE-FIM in two distinct roles. One as an IdP (specifically the User Management set of services within SCS) and additionally, in a new role within the EE-FIM as a Dependent Service of a Relying Party. It was agreed that a set of existing SCS functionality would be implemented as discrete, stateless REST services that Relying Party web applications invoke on the behalf of an EE-FIM user.

[1] *Note: EE-FIM Partner access to other SCS services (other than user management and registration) will use a similar procedure.*

This necessitates that SCS be provided with RESTful interfaces by the EPA SCS Team to enable it to function smoothly within the EE-FIM network. All the participants decided that this was the necessary and logical approach. Additionally these stakeholders concluded that for the User Management set of services, EPA SCS Team will make the necessary modifications for that set of services to be able to operate as a standard IdP within the EE-FIM context, if that is possible, or else determine how SCS works as an IdP outside of the standard process.

How the SCS Works As a Dependent Service Under EE-FIM

Under the Dependent Service scenario, the SCS are accessed via the RP (a partner web application such as NM AEIR, Air Emissions Inventory Reporting, or ND ERIS, Electronic Reporting Information System) who has established their own access to SCS. This RP (the partner web application) presents to the user a UI that the user may input the information required for the SCS API depending on which components of the SCS the RP implements.

The RP, as typical under EE-FIM, controls authorization and checks the authentication of the user. If the RP implements SCS functionality into their site additional user verification steps are required. The RP will need to evaluate the LoA of both the user and the user's authenticating IdP by examining the user claims provided by the EN Enterprise Security Bridge. If the user's authenticating IdP does not have the required LoA -- for example, if the CROMERR minimum LoA is not met -- the RP returns a set of links to IdPs that meet the LoA criteria necessary (i.e. a list of CROMERR Compliant IdPs). The RP can then require the necessary two-factor authentication from the CROMERR compliant IdP in order to proceed with invoking the SCS REST services that are part of the RP application functionality. For example, a partner's emissions inventory application (RP) collects the emissions from the user and upon invoking an SCS REST call such as for signing or for storing the CoR the RP authenticates the user using two factors via EE-FIM IdP.

Again as typical under EE-FIM, the RP is responsible for evaluating the user claims from the authenticating IdP for the purposes of authorization and evaluation of the LoA. The RP will likely need to be responsible for the record retention and audit trail needed to maintain CROMERR compliance depending on the set of SCS services involved in the transaction.

Below (*Figure 5*) is a proposed process flow diagram for how the utilization of Shared CROMERR Services would work as Dependent Services under a Relying Party.

A number of questions remain about how the Dependent Service model will operate, such as how SCS is "integrated" with EE-FIM if it is not taking an active role in utilizing IdP claims for the user. These questions will need to be addressed in any future extension of this work, and will be part of the ongoing effort in partnership with EPA to implement EE-FIM.

SCS References

The EPA's Executive Summary of SCS

EPA SCS Integrated Project Team page

EPA SCS Overview

NMED Google Drive Collection of SCS Resources

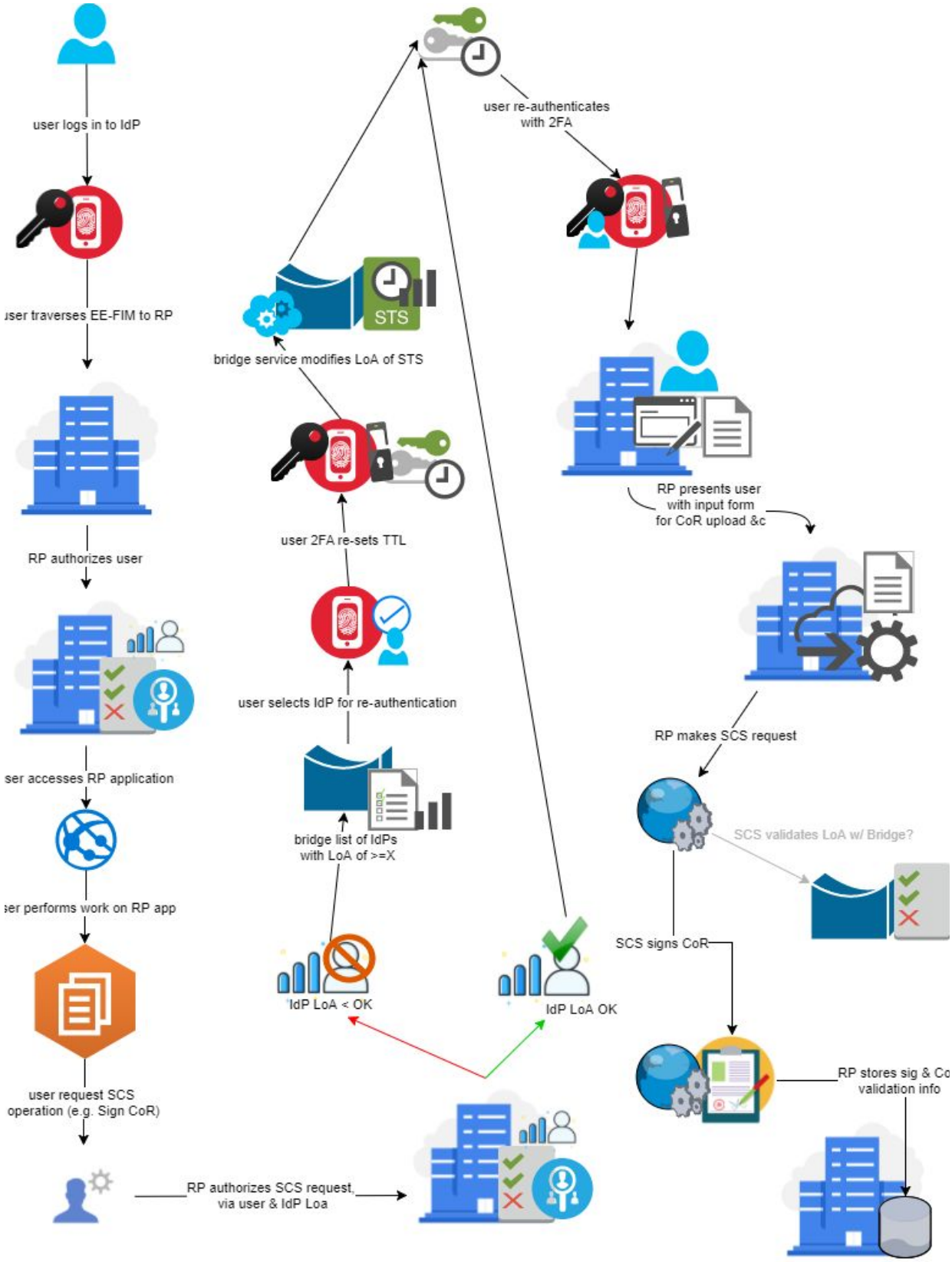


Figure 5: SCS as Dependent Service EE-FIM process flow

The Benefits of Integrating SCS with EE-FIM

There are potentially several compelling benefits to a Federated Identity System in regards to the US EPA's Shared CROMERR Services.

EE-FIM Facilitates Access to Shared CROMERR Services

For the end user such as a worker for a regulated facility, authenticating with an IdP registered with EE-FIM and is CROMERR compliant allows them to traverse between emissions reporting tools whether hosted by a partner state, a tribal emissions reporting tool, or an EPA reporting tool without having to maintain separate identities at each site for which they are required to report based on jurisdiction and delegated authority requirements. The fewer identities to manage, the fewer errors; the fewer passwords to remember, the more accurate and consistent the user attribute information is across the system.

For the co-regulator partners, Shared CROMERR Services integration with EE-FIM provides flexibility, burden reduction and more reliable security. For example, states and tribes that do not currently provide identity management at the CROMERR-compliant level can implement Relying Party integration for their web applications requiring CROMERR compliance, and rely on the EE-FIM for two factor identity proofing. Additionally, states that do provide CROMERR compliant authentication and identity management may still want to use the SCS Copy of Record (CoR) or SCS signing ceremony for electronic signature of documents. Also, partners may want to facilitate their identity proofing process by invoking the SCS identity proofing service, LexisNexis, to augment their existing identity management capabilities.

By providing SCS as discrete invokable REST services to trusted Relying Parties on the EE-FIM network, enhanced access, traversal, security and functionality can be incorporated in a flexible, as-needed basis to existing partner and EPA web applications.

Addressing Partner Perspectives and Concerns with SCS and EE-FIM

North Dakota

North Dakota is familiar with SCS but had not been paying it much attention. Primarily they are interested in the possibilities of easy access to the SCS Identity Proofing set of services and what that could provide to them. It was very important to them that they be able to maintain control of authorization provided to users on the system, which the RP + Dependent Service model supplies. They had concerns about how the signature piece would work in the absence of a single Federal user ID, which subverts the EE-FIM concept. The Dependent Service approach should address this concern ably, as the signature is associated with the EE-FIM user via the

RP's access to SCS, keeping the signature associated with the Relying Party providing the service to the user.

Wyoming

Wyoming has their own CROMERR-Certified solution - ENVITE - and had their CROMERR application approved in 2012 and so is very familiar with SCS. Like North Dakota, the LexisNexis Identity Proofing set of services has the most appeal for them, though they are intrigued by the possibility of the Signature and Copy-of-Record set of services if they could be leveraged for uses outside of CFR-40. They are currently in need of a replacement to Sharepoint for this purpose. These needs are sharpened by the loss of their Sharepoint administrator and the fact that their affidavit process is physical-mail-based and therefore slow and labor-intensive. Since the ENVITE application is REST-based, one of their primary concerns was that of communication with the SOAP-based SCS -- something which the next steps coming out of the SCS / EE-FIM meeting in Washington DC directly address. Another concern is the ownership of Signed Documents, especially for those entities that don't have the resources to host such themselves. This concern is another that the Dependent Service model addresses directly by keeping that ownership with the Relying Party providing access to the CoR service.

Agreed-Upon Next Steps

The following action items resulted from the August 29 & 30th meeting at the EPA Headquarters West Building in Washington DC where the NM team met with EPA OEI staff and consultants. The primary topic discussed was integrating Shared CROMERR Services (SCS) with the E-Enterprise Federated Identity Management (EE-FIM) system. The ND and WY state partners were briefed during a segment of that meeting.

1. **Integrate SCS as an IdP** The OEI Shared CROMERR Services (SCS) team will work with the OEI Identity Bridge team to integrate the identity management component of SCS with the Identity Bridge as an Identity Provider . This integration will result in providing a SCS login to users as an option for authentication within the E-Enterprise Federated Identity Management (EE-FIM) system. Web applications that are registered as Relying Parties within the EE-FIM (all Relying Parties must be registered with the Identity Bridge) will only accept local tokens and tokens issues by the Identity Bridge and if no such token is present the Identity Bridge will present a list of registered Identity Providers which will include Shared CROMERR Services as an option after the integration has been completed. NM and other state partners will assist with testing this new IdP to verify consistent functionality.

2. **Stand up REST SCS Services as Dependent Services to an RP** The OEI SCS team will develop REST interfaces that provide a set of existing SCS component functionality as discrete, stateless, decoupled services. The interfaces discussed included: Identity

Proofing via LexisNexis, detached signature and secure storage for Copy of Record electronic documents. The SCS team has already drafted a project within OEI for this purpose. NM and other state partners will participate at junctures during the project execution to verify objectives, requirements, design principles and assist with testing. As part of this effort, the topic of establishing trust between a registered Relying Party within the EE-FIM and a dependent service such as SCS REST Services will be analyzed and evaluated. Recommendations to address this new concept may need to be presented to a governance committee for evaluation and determination.

3. **Standardize user claims** There was general consensus that there is a need to standardize on a minimum set of user claims that the authenticating IdP provides to the Relying Party. The set of claims is needed so the Relying Party has enough information to know whether the user has been authenticated with a Level of Assurance adequate to perform certain functions within the web application. The set of claims also provides unique identifying information to link users with local identity management systems and user registration information. To meet SCS requirements, Level of Assurance information is particularly important. A standard way to represent these user attributes as claims by the Identity Provider is needed, and should be addressed through a governance group. A recommendation for a EE-FIM governance group that includes representatives of the participating entities is currently being drafted for consideration by the E-Enterprise Quad Chairs.

4. **Security Bridge modifications** Based on the scenarios discussed in DC it is likely there will need to be some modifications to the Bridge. The claims mapping code may need to be revisited to ensure consistent formatting of claims processed by Relying Parties. Also, the RP may need to request a list of IdPs from the Bridge that meet or exceed a certain threshold LoA in order to allow the user to proceed within the RP application. This is needed because a Relying Party evaluates the LoA of the IdP the user authenticated with vs. the minimal LoA requirement of the Relying Party, in order to allow access to the application the RP provides. If the user LoA is insufficient, the Bridge must provide a list of those IdPs that *do* meet that LoA requirement. This IdP list functionality currently does not exist.

5. **Analysis on Security Requirements for new role "Dependent Services to RP"** Depending on the results of additional analysis as the SCS integration work proceeds, there may be additional modifications to the ID Bridge. One such area that may result in some modification is a need for SCS to trust the Relying Party (web application that calls the SCS web services) and to be able to derive the associated tenant in order to authorize access to various SCS components. SCS currently has a mechanism to do this and it may be easily applied with the newly created set of REST services as well, however, there may be an opportunity to leverage some capability currently in use around the RP registration process with the ID Bridge.

6. **Onboarding Documentation** - One of several requirements for a production-ready system is the need for complete and accurate technical documentation. This documentation must be readily available, consistent, address multiple platform integration issues and be maintained over time as modifications and changes are introduced within the infrastructure of the EE-FIM system. EPA OEI has begun the process to hire contractual technical writers to establish a set of documents for partner states to use for onboarding RPs, IdPs and dependent services to RPs. Some documentation exists which should be revisited for accuracy and completeness and some missing documents will need to be created.

7. **EE-FIM Governance** A governance group needs to be established to address a host of issues such as standard claims, on-boarding requirements, security notifications, recommendations for a sustainable support model and many other topics, and including change management. This last would be a process that evaluates and notifies members of changes to the production environment, whether it is to the Bridge, partner systems or EPA systems that have the potential of unexpected consequences to users within the system. Chuck Freeman from EPA OEI and Mary Montoya from NM Environment Department will make a proposal to the E-Enterprise Quad Chairs for a long-term governance group to be established that will take up these and future topics pertaining to the operations of the E-Enterprise Federated Identity Management (EE-FIM) system.

Recommendations & Continued Work

EE-FIM & SCS Integration, Recommendations & Next Steps

A more complete discussion of next steps towards EE-FIM implementation can be found in *Appendix E*. Those conclusions are included in an abbreviated fashion here, but are also expanded upon in the identified next steps that came out of the SCS integration meeting.

Identity Provider (IdP) Recommendations & Next Steps

As mentioned above, it will be necessary early in the EE-FIM implementation process to standardize the set of Identity Claims per mutual agreement among all Partners in the federated trust framework. This standardized set of claims should consist of the minimum claims needed for the technical operation of the framework, augmented with the minimum claims needed for efficient governance of the system. A more complete listing of these claims is found in *Appendix E*, but they would include a unique identifier for the user to be used as a federated ID, such as email address, additional user attributes useful to contribute to the RP authorization decisions such as organization and items related to governance such as Level of Assurance (LoA). Significant additions to the necessary claims that came out of the SCS Integration meeting in Washington, DC identified the inclusion - by the IdP - of user LoA, IdP LoA, and Time-to-Live (TTL) for the authentication piece of the token.

The Bridge's Attribute-Mapping (claim-mapping) feature should be used, and possibly extended to enforce the standardization of identity claims across all the IdPs in the EE-FIM system. Additional IdP-specific claims can still be allowed, such as, for example, Shared CROMERR Services registration information. However, the core claims should be standardized to reduce the burden on Relying Parties (RPs) as much as possible. During the integration efforts of the ISOL proof-of-concept project each RP had to write additional code to handle the differing identity claims from different IdPs. This burden would only increase as new IdPs were added to the EE-FIM framework, unless standardized claims are mandated. In the big-picture sense, this will ensure that the EE-FIM system remains scalable.

Relying Party (RP) Recommendations & Next Steps

There are several recommendations for the RP, many of which also revolve around the standardization of claims. RPs must use these claims in a standardized manner, for instance they must use the email claim as the federated user ID. The RP must be able to rely on a unique identifier within the claims in order to lookup the user in their system to determine what the user is authorized to do within their application.

The RP must also utilize LoA information from the claims properly to know whether the user would be required to login using a different IdP to meet the RP identity proofing requirements.

As the use of REST services are incorporated into the trust framework as “Dependent Services to an RP” (a new role within the EE-FIM) the RP client may need to provide some identifying information to the REST service to ensure that the request is coming from a valid partner RP. Many of the details on how secure REST services will be implemented within the EE-FIM are yet to be determined. Changes to the process used to register RPs to the EN Security Bridge may need to be hardened to ensure the RPs membership in the EE-FIM and to provide identifying information to the REST services.

EE-FIM governance should establish Partner agreements that include guidance on how RPs can best utilize claims to support authorization decisions in an appropriate and standardized manner. Since authorization is in the hands of RPs, a consistent reference framework for how authorization should be handled by an RP would be a valuable tool.

EN Enterprise Security Bridge Recommendations & Next Steps

As recommended above, the EN Enterprise Security Bridge’s claim-mapping feature should be used for both the standardization of all EE-FIM core identity claims and the mapping of the claims provided by external IdPs such as Google, Facebook etc. to EE-FIM specific token claims -- which themselves need to be standardized. Discussed previously, and in *Appendix E*, standardization of claims reduces the burden for RP integration by easing access to user attributes for authorization determination and access to identity-proofing capabilities of the IdP by way of the LoA information. There may be a need to extend the capabilities of the Bridge to enable it to serve these critical functions.

Regarding external IdPs such as Yahoo, Microsoft, etc.the Bridge should be configured to map the LoA of social network IdPs with either no LoA or one of 0 (the lowest LoA value).

The Bridge may also need to be modified to provide a list of IdPs based on LoA value to further facilitate Relying Parties ability to enforce a minimal level of LoA for access and/or two factor authentication from an IdP.

The ability for users to traverse smoothly from one Relying Party (RP) to another without needing to re-authenticate is an expected and desirable function of a Federated Identity Management (IdM) system. The project team produced a white paper titled, “EPA Identity Bridge – Proposal for Federated Single Sign On”, that the NM project team presented to OEI. That document has been provided as *Appendix D* for reference.

The EPA’s Identity (ID) Bridge system was designed to support ‘active’ traversal and partially supports ‘passive’ traversal. ‘Active’ traversal requires Relying Parties to explicitly code for each traversal path between Relying Parties, whereas, ‘Passive’ traversal does not require that Relying Parties have an active role in the traversal of the user to other Relying Parties, therefore, no coding specific to user traversal is required. The Bridge will need to provide some

additional endpoints to fully implement 'passive' traversal. This traversal approach has been tested out in coordination with the Bridge team and it works as expected.

The Bridge needs to include additional URL endpoints in support of passive traversal within EE-FIM. In short, the issue is that there is a need to validate[2], remove or renew session cookies that can only be read by the cookie owner, the Bridge. Redirecting URL endpoints are necessary to provide these cookie services to the EE-FIM. This issue is discussed in depth in *Appendix D*.

Governance Recommendations

The E-Enterprise (EE) Shared Identity Management Concept of Operations (June, 2015) and the email sent to the E-Enterprise Management Board on July 14, 2017 (see *Appendix E*) identified several areas where ongoing governance would be required to sustain a production-level trust network among partner entities. In the course of this grant project several of those topics came up as well as a few additional ones. As will be evident from the issues raised below, it will be necessary to establish and populate an EE-FIM Management or Governance Board. The recommended EE-FIM governance requirements for moving to a production system comprise three broad categories: Operations & Support Procedures, Standards & Policies, and Research & Development.

Operations and Support Procedures

Change Control Process - A Change Control Process needs to be established that ensures communication and participation by all EE-FIM partners in modifications and maintenance of the software components distributed throughout the system that have a potential impact to users in regard to service delivery.

Notifications - A mechanism for notifications needs to be established. Example communication include: new or removed IdPs and RPs, security alerts, scheduled outages for maintenance, approved change control announcements

Tech support - A means for users, both end users and IdP and RP owners, to report a problem and receive technical support for issues relating to the EE-FIM network. Much of this is currently handled by EPA staff dedicated to the task, but the additional load on the Bridge system that EE-FIM traffic could pose might make it necessary to supplement current Bridge support staff under the EE-FIM rubrik.

Partner forums - A collaboration tool to facilitate communication among partners regarding integration issues, policy issues, connectivity issues, design approaches and other areas of interest or concern concern with EE-FIM. Additionally, a repository of integration code and

[2] Validation functionality has already been implemented and tested

technical documentation would also be very useful. This forum should also be configured to host peer-sourced troubleshooting and provide mutual support. Preferably this support infrastructure would also include an EE-FIM knowledge base as well as a repository of integration code and a system status map/dashboard indicative of the overall health of the network and the number and approximate geographic location of IdP and RPs that are active on the system.

Usage metrics - A means to provide to members of user activity on the network.

Partner training - Provide a means for online training opportunities for partners to understand integration options and potential benefits of participation.

Outreach - Continually monitor member participation and usage statistic and actively reach out to state, tribes, local governments and other EPA programs to encourage participation.

Standards and Policies

IdP Standards - Development of a set of standards and responsibilities to meet the requirements for this role.

RP Standards - Development of a set of standards and responsibilities to meet the requirements for this role.

Claims and Secure Token Standards - Identification of the minimum set of standard claims an IdP must provide and the additional set of claims required to meet other criteria such as specific identity proofing Levels of Assurance (LoAs) and CROMERR. Also change is inevitable and there will be a need to revise or amend the set of token claims, or possibly the structure of the token itself. A governance system will go far toward preventing, or at least mitigating, disruption to the Federated trust system caused by the necessary evolution of the token and its set of claims.

Bridge Guidance - Similar to Claims, the Identity Provider protocols supported by EE-FIM could someday change or be amended. A governance process should be positioned to approve, plan and regulate such modifications to the supported EE-FIM transport protocols in such a way as to minimize the potential disruption of the trust network

Partner Agreement Policy that outlines terms of engagement with the EE-FIM network and defines the security and verification requirements for participation in the trust network as an IdP or RP. This document should include a process and rules for terminating a participating partner for reasons ranging from abrogation of partner responsibilities (including security obligations) to state level organizational changes.to include process and rules for terminating a partner

Partner Adoption Strategy to include onboarding process and assessment. Such a strategy would include a defined means and method for the collection of metrics of trust network participation as well as the process for setting EE-FIM adoption goals.

Security Incident Response Policy to include an emergency process for removing potentially bad actor identities from the network

Vendor Certification - A continuing necessity that the Standards and Policies group should also fulfill is the maintenance and publishing of an official EE-FIM-endorsed list of certified vendors for partner integration work.

Research and Development

Continuous Improvement Process - At periodic intervals, assess existing performance and identify new features to improve the system

Secure APIs or Dependent Services to a Relying Party - Investigate ways to leverage the Bridge and Secure Token Services to secure APIs used between partner systems for programmatic data, document and map sharing

Shared CROMERR Services - While some of this work has begun it is important to continue to investigate ways to leverage the Bridge and Secure Token Services to secure APIs used between partner systems for programmatic data, document and map sharing

Third Party Relying Parties - Investigate ways to integrate third party collaboration tools as Relying Parties into the system such as Google Docs and Sharepoint to promote increased secure collaborative work between co-regulators and the regulated community.
Other public sector IdPs - Investigate ways to integrate other IdPs within other trust networks such as the public University system's federated identity management Identity Providers.

New Features and Enhancements - Actively research current industry trends and technologies to insure that the the system stays aligned with contemporary Open protocols and encryption and other industry standards.

Summary

The EE-FIM project was the result of an EPA Exchange Network Partnership Grant whose intent was to work with three state partners to test out the technical viability of integrating with the EPA developed Enterprise Security Bridge to implement a working proof-of-concept of a federated system for identity management. This federated system is secure, elastic, straightforward to adopt, robust, adaptive and flexible.

The project team, with considerable effort, was able to overcome numerous challenges, both technical and conceptual in nature, in order to realize a working demonstration of a federated identity management system with truly distributed, independent systems. The working demonstration included verification of seamless traversal for an authenticated user from one independent system (e.g. NM Air Emissions Inventory Reporting web application) to another (e.g. E-Enterprise Portal) and to another (e.g. North Dakota's Environmental Reporting Information System). The team started by evaluating the foundational architecture established by the EPA-developed Security Bridge (see *Appendix A*). The team verified that it was built using open standards "claims-based" technology for identity management including defined roles using the terms seen so frequently in this document, "Relying Party" and "Identity Provider" (see *Appendix B*). The goal for the team was to leverage and utilize as much existing Identity management architecture among the partners as was possible given this existing central broker component (the Security Bridge).

The team soon realized that a basic challenge would be interoperability between partners based on different technology stacks, such as the Java-based architecture of NMED vs. the .NET web application framework foundation of North Dakota. To solve this issue, the team researched the capabilities of the Windows Identity Framework (WIF) the foundational technology on which the Security was developed. The key to integrating the partner state systems in the least disruptive manner resided in the inherent functionality of the WIF. The WIF supports passive token creation and verification by writing a cookie accessible only by the Bridge in the user's browser. Through the common practice of redirects for creation and verification of tokens, used by many web identity frameworks (such as OpenID Connect) and supported by WIF as well, integration with dissimilar technical platforms of the state partners was greatly simplified. See *Appendix C* for the technical details of the state partner integration process.

Use of the Bridge as a central translation hub for the security token in this manner has both pros and cons. It is a single point of failure for an otherwise distributed network but it makes it possible for diverse Identity management technologies to interact seamlessly. To illustrate this latter point, NMED used open-source libraries to communicate with the Bridge, while North Dakota and Wyoming could both leverage the fact they shared the same underlying technology as the Bridge and connect via a configuration-only approach. Both integration approaches do require significant, albeit minimized, local changes to link identity stores, gather additional registration information, and/or customize authorization management given an expanded user base.

After the project team had worked out the initial hurdles of the basic architecture and functionality of the federated system, many additional months were spent to establish the partner's presences on the system. This length of time was necessary due to the need to identify and document the technical starting point of each partner, which took place primarily during a series of Discovery Sessions held on-site with representatives from each partner (see *Appendix C*).These sessions provided the information necessary to develop a gap analysis for each partner which then could inform the team decision as to which EE-FIM integration options

was the best fit for each role of IdP and RP on the system. For all three partners in the Proof-of-Concept implementation, the WS-Federation Passive Requestor Profile was the chosen means for establishing a Relying Party presence on the federated network. For Identity Provider, Wyoming and New Mexico chose the OpenID Connect (OIDC) protocol, utilizes IBM Tivoli via LDAP for external users and Active Directory for State employees for their Identity Management. Future partner integrations might provide opportunities to utilize options other than those used above as necessary.

While the initial partner onboardings took some time, this was largely due to the initial analyses necessary and will decrease exponentially as the onboarding process is rehearsed, documented and transferred to an operations support model.

In the case of the EPA, the discovery sessions revolved more around the capabilities and advantages of the Bridge, along with more general discussions regarding what later became the EE-FIM network, including LoA, Secure Token Services and the EPA's prior experience in federated identity management.

Once all the details had been worked out, encryption keys (a.k.a. "thumbprints") exchanged and partners integrated onto the nascent E-Enterprise Federated Identity Management System, the project team gave a presentation on the architecture and partner implementation at the 2017 Exchange Network Conference in Philadelphia, PA on May 16th, 2017. A video of the presentation can be found at this link. The presentation powerpoint slides can be found at this link.

The presentation took the audience through the entire life of the project from initial goals to hurdles encountered, through lessons learned as well as overall project experience and culminated with a live demonstration of a working prototype. All partners were represented at the conference and shared their experience on the project. The presentation was well-received and generated much interest from conference attendees. A frequently-asked question was how this work relates to EPA's Shared CROMERR Services which led the project team to further explore that particular topic.

The exact nature of the integration of Shared CROMERR Services with the E-Enterprise Federated Identity Management System prompted much head-scratching from the team over the course of the project. It took many whiteboard sessions, several phone conferences and finally a two-day, in-person meeting with the SCS team in Washington, DC before a detailed process flow of how SCS integration with EE-FIM could be definitively mapped. The solution finally agreed upon included the creation of what is essentially a third role on the EE-FIM network, that of SCS as Dependent Service to a Relying Party. This scenario presupposes that an established RP is the entity that provides access for EE-FIM users to SCS, via a traditional SCS implementation. While additional and complex questions remain regarding this approach (as well as augmentation of SCS in order for it to work seamlessly), this solution provides the most straightforward usage of SCS on the EE-FIM. It utilizes SCS's least complex and most

accessible functionality, places the authorization and tracking burden on the RP providing SCS access[3] and preserves CROMERR-compliance for the entire process which is the most logical and lease cumbersome of the potential approaches.

As a result of the work that was done in the EE-FIM project, a set of recommendations for further development of the system has been identified. It includes recommendations for additional technical work that must be done to address identified issues, answer outstanding questions and for needed governance infrastructure to support the continued effective operation of the the federated system. See *Appendix E*.

Broadly, the governance needed falls into the categories of Operations and Support, to troubleshoot the network itself as well as provide support to users of existing and prospective federation members; Standards and Policies, to determine the answers to necessary operational questions such as the standardization of token claims as well as regulate the operational behavior of the federation; and Research and Development, to streamline processes and pursue the continued positive evolution and relevance of the network .

This undertaking of establishing a Federated Identity Management platform usable by the EPA, all fifty states and potentially Native American Sovereign Nations or other municipal entities is a complex matter. A single two-year project with a handful of participants, all of which have other unrelated responsibilities, still leaves some details unexplored and questions unanswered. To fully establish an operative system will require additional effort. That being-said, this project team definitively proved that a system capable of providing a user a seamless traversal experience across multiple partner systems and applications, up to and including use of Shared CROMERR Services, is possible. The team established such a system, which included a total of three partners in a mix-and-match of IdP and RP roles with EPA involvement as a fourth participant via the EN Enterprise Security Bridge's role as the provider of security tokens. Users were able to login via one IdP and traverse easily to RPs elsewhere within the network. The next steps needed are to grow the existing Proof of Concept system into something that is fully operational and providing public benefit to a wide community of users.

[3] Except in cases where the RP is utilizing SCS User Registration & Identity Management Service for authentication, in which case SCS handles this authorization and tracking

Appendix A: Technical Details

To begin the EE-FIM feasibility analysis project, NMED's research team met with the EPA's Exchange Network (EN) Enterprise Security Bridge team from the Office of Environmental Information (OEI). This was the first step in understanding what the evaluation and implementation strategy would include. The Bridge was already in production use, providing federated identity management (FIM) services to EPA web applications, most notably the EPA's E-Enterprise Portal. NMED learned about the components of the prospective federated identity management approach using the Bridge as a centralized secure token broker between identity providers (IdP) and relying party (RP) web applications. This was accomplished by use of the WS-Federation trust framework standards along with a secure token services (STS) implementation, using SAML2-based security tokens. The Bridge team explained the technical processes that would be needed for each state partner to integrate with the Bridge as an IdP and as an RP. The NMED team came away from these sessions with a much better understanding of the EN Enterprise Security Bridge and the role that it could play in the system as a whole.

The EPA Enterprise Security Bridge

Over several phone discussions and one in-person meeting, the NMED EE-FIM team met with EPA Enterprise Security Bridge personnel to understand the architecture and capabilities of the Bridge. They were able to develop a deeper understanding of what the functionality has to offer, how it works and how it fits into an EE-FIM implementation. The results from this data-gathering are presented and described in detail in this section.

EPA – Identity Management (IDM) Bridge and Secure Token Services (STS)	
Microsoft Windows .NET Environment	
Identity Store	For EPA Exchange / NAAS IdP: Active Directory Federation Services (ADFS) 4.0
Identity Framework	WS-Federation and WS-Trust via Microsoft Windows Identity Foundation (WIF) API – version WIF 4.5, which is now part of Microsoft .NET 4.5 Framework
Bridge / Server	.NET 4.5 Framework, MVC 4, Web API and WIF
Bridge Protocols – Internal	OAuth2, OpenID, Live ID, Attribute eXchange (AX), Microsoft Web Browser Federated Sign-On Protocol (MS-MWBF), WS-Federation 1.2, WS-Trust, SAML 2.0

Bridge Protocols – for Identity Provider (IdP)	OpenID (e.g. PayPal), OpenID+AX (e.g. Yahoo), Live ID+OAuth2 (e.g. Windows Live ID), OpenID Connect / OIDC (e.g. Google), WS-Federation 1.2, WS-Trust
Bridge Protocols – for Relying Party (RP)	SAML 2.0 Assertions and Tokens. EPA custom SOAP-based Web Services API
Bridge IdPs	Facebook, Google, Twitter, Windows Live, Yahoo!, NAAS, CDX
Secure Token Service	WIF 4.5
Identity Token Protocols	**IdP**: SAML 1.1/2.0, JSON Web Tokens (JWT - *for OIDC*). **RP**: SAML 2.0
Identity SSO Authorization	ASP .NET membership, roles and profile.
Identity SSO Claims	**Note 1**: varies with the IdP – *Example for OpenID/AX is*: email, name, namePerson, securityToken, authenticationMethod, authenticationInstant **Note 2**: varies by *claimRequirements* configuration – see Bridge docs.
.NET Relying Party (RP)	Integration via WIF. Modify .NET IIS web server configuration and *web.config* file. Modify RP code for full integration with identity store and for RP traversal.
Java Relying Party (RP)	Modify RP code. **WS-Federation**: via 3rd-party API such as *auth10* or *Apache Fediz*. **SAML 2.0**: via 3rd-party API such as *OpenSAML*, *Spring Security SAML*, or *PicketLink*.
PHP Relying Party (RP)	Modify RP code. **WS-Federation**: via 3rd-party API such as *SimpleSAMLphp*, *ACSFed,* or *Auth0*. **SAML 2.0**: via 3rd-party API such as *SimpleSAMLphp*, *LightSAML*, or *OneLogin*.
Generic Relying Party (RP)	Modify RP code. Use custom EN Enterprise Security Bridge SOAP-based Web Services API.
Operating System	Windows Server 2012 R2 Datacenter x64
Web Server	Microsoft IIS 7.5
Web App Framework	Microsoft .NET Framework 4.5
Web App Language	C# .NET
Database Server	Microsoft SQL Server 2012 R2

Firewalls	Application-level firewalls for internal and external users. Ports 80 and 443 open.

Table 9: EPA Bridge Discovery Session Summary Questionnaire

The Bridge utilizes and implements the WS-Federation protocols and standards for federated identity management (FIM), which provides the ability for IdPs and RPs to participate within a trusted ecosystem. The Bridge was programmed using Microsoft's Windows Identity Framework (WIF), which is the technology component that provides - among many other services - the WS-Federation implementation. WS-Federation standards and their realization within the WIF library provide for both *active* and *passive* validation protocols for relying parties (RPs) in the trust framework. Active validation is implemented by a relying party by invoking a SOAP-based web service, while passive validation is performed by the relying party by issuing a web redirect to a validation endpoint of the Bridge. See section "Traversal and Single Sign-On (SSO)" for more details on active version passive WS-Federation standards and protocols.

The EN Enterprise Security Bridge's Multi-Protocol IdP Manager

One of the primary features of the EN Enterprise Security Bridge that sets it apart from other IDM systems is its Multi-Protocol IdP Manager. This subsystem allows the Bridge to support a heterogeneous mix of IdPs from the various state and federal partners, as well as commercial IdPs from companies such as Facebook and Google. It supports a wide range of both open IdP standards as well as proprietary standards (e.g. Facebook). The supported IdP security token and authentication protocol standards include OAuth (1 & 2), OpenID (1 & 2), SAML (1 & 2), OIDC (OpenID Connect, an authentication layer on top of OAuth 2.0), and Facebook. This covers about 98% of the IdPs in use today.

There are two primary security token standards used by these IdP systems: SAML tokens that use an XML format and JWT tokens that use a JSON format. SAML is the abbreviation for Security Authentication Markup Language and JWT is the acronym for JSON (JavaScript Object Notation) Web Token. Note that JWT is pronounced "jot".

No matter which IdP the user chooses to login with, Bridge's Multi-Protocol Manager will always convert the authentication token into SAML2 format and "transform" the protocol into WS-Federation protocol. This is important because it means that the relying parties (RPs) connected to the Bridge will only ever have to implement a single protocol and only have to process a single security token format.

Rather than "transforming" the protocol, It is more precise to say that the Bridge communicates with each IdP via the IdPs "native language" - i.e. communication protocol standard. Further, the Bridge acts as a middle-man or identity broker, because it then communicates with all of the

RPs via the single WS-Federation protocol - which uses the single standard of the SAML2 security token to contain the user's identity claims information.

More information about the details of the WS-Federation protocol can be found here:

The complete EPA Discovery Minutes can be found here.

The EPA vision for the Trust Framework is described in more detail in this document.

Technical Details of IdP and RP Roles

The EE-FIM trust framework utilizes industry standard technologies to provide secure login services and single sign-on (SSO) ease and convenience for a heterogenous network of federal and state environmental web applications, gateways, and services. The key web and internet standards and protocols include:

- HTTPS (secure web HTTP communication protocol)
- HTTPS web redirect standards and protocol
- Web data persistence via secure browser cookies
- WS-Federation federated identity management (IDM) standards and protocols
- Secure Token Services (STS) using Advanced Encryption Standard (AES)
- Authentication data encoding standards: SAML (Secure Authentication Markup Language) and JWT (JSON Web Token)
- OAuth, OIDC, and SAML authentication protocols
- Windows Identity Foundation (WIF) API library for WS-Federation and federated IDM

In the case of web applications, WS-Federation and WIF specifically provide for a passive validation mechanism *because **web browsers*** - implementing only standard HTTPS protocols - inherently do *not* have the ability to invoke an active SOAP-based web service. Passive validation is accomplished by utilizing the technologies of HTTPS, web browser security, web application redirect protocols, encryption, secure STS tokens, and secure web cookies. Below, is an explanation and examples of how these all work together for validation.

IdP Authentication Details

When a user first accesses an RP (web application or gateway) in the EE-FIM trust framework, the RP will provide a link or redirect the user to the login screen of the EN Enterprise Security Bridge. When this user selects their desired IdP from the Bridge's login page, the Bridge performs an HTTPS web redirect to send the user to the login page for that IdP. The user then logs in by entering their credentials for the *account they have registered with this IdP*. The IdP then authenticates the user by checking the username and password against its identity store database.

Upon successful authentication, the IdP will then create a signed, encrypted security token in its native format and post it back to the Bridge via its native protocol. Next the Bridge's Security Token Service (STS) will convert the IdPs native security token format to to a SAML2 security token, and sign it *with the signature of the EN Enterprise Security Bridge*. Lastly it will post this STS token back to the RP that the user originally accessed, along with a login success message.

IdP and Secure Tokens - Behind the Scenes

Whenever a user logs into the EE-FIM using an IdP integrated with – and hence, trusted by -- the EN Enterprise Security Bridge, the Secure Token Service (STS) component of the Bridge generates an STS security token. It *also* generates a secure cookie (or multiple cookies, which is commonly needed due to cookie size limits) that contains the signed and encrypted STS token. Thus, after an IdP login, the STS cookie(s) are written into the user's web browser cookie store by the Bridge itself and "tagged" with the web URL of the Bridge. Because of fundamental web browser security that implements the HTTPS protocol and secure web cookies, this "tag" ensures that the *cookie can only be read by the EN Enterprise Security Bridge*, and *cannot be read by any other web application*, such as an IdP, originating RP or another RP. The browser will not let any of them read the STS cookie(s), and due to the signing and encryption, not even the user can read the contents of these STS cookie(s).

RP Validation Details

Because the process of IdP login and generation of STS cookie(s) is automated and occurs separately and apart from the RP, the validation burden on the RP is greatly reduced because the RP only needs to passively perform an HTTPS redirect to the URL of the validation endpoint of the EN Enterprise Security Bridge. When the Bridge processes this RP validation redirect, it first checks that the RP is registered with – and hence trusted by -- the EN Enterprise Security Bridge. It then reads the STS cookie(s) from the user's browser.

It's worth noting again that the Bridge is reading the STS cookie(s) that it itself had written in the user's browser sometime earlier in the day during the process of an IdP login. Also recall that *only* the EN Enterprise Security Bridge can read the STS cookie(s) due to intrinsic web browser security surrounding cookies and their domain of origin.
The Bridge then decrypts the STS cookie(s) using its own private key to retrieve the STS token. Lastly, the Bridge validates the STS Token (which, again, was issued earlier via IdP when the user logged in) by using the public signing key of the IdP that was used during the user's login. At this point, the user is now validated - verified to have logged in earlier via registered IdP. Now it is up to the RP to authorize the user and grand appropriate access to resources.

RP Claims Processing

After the EN Enterprise Security Bridge completes the STS token validation process it performs an HTTPS POST action back to the RP (at it's Bridge-registered return endpoint) with a SAML assertion containing the identity claims provided the IdP. It is then the RP's responsibility to verify and decrypt the SAML assertion (using the EN Enterprise Security Bridge key shared with the RP), parse the XML data contained the SAML assertion, and process the identity claims data. The identity claims will contain a user ID (email address), which is the database key that will allow the RP application to check its user database and grant the appropriate access to resources managed by the RP web application. A topic for future EE-FIM governance will be to standardize the required set of identity claims across all of the IdPs in the trust framework.

Traversal and Single Sign-On (SSO)

Seamless and natural traversal of RPs within the EE-FIM trust framework is made possible and manageable due to the passive validation system of the EN Enterprise Security Bridge. *This is one of the key benefits of a federated IDM system*. These features are enabled because the Bridge was designed and implemented using the underlying technologies of the WS-Federation standards and protocol, along with the WIF technologies which implement these standards and protocols. The key factors enabling the seamless traversal are the WS-Federation Passive Requestor Profile, and the small extension to this standard implemented by the Bridge. This extension was the capability of the validation endpoint to return an error message if the user is not validated. This ability to traverse from RP to RP, after logging in only one time via an IdP is also referred to as a Federated Single Sign-On (SSO) System.

The traversal is also possible via an active-SOAP mechanism, in which the Relying Party captures the Security Token from the SAML assertion, and validates the token with a SOAP call to the Bridge by invoking the "Validate" method. None of the parties chose this option because of the overhead to implement it, which includes having to build the active links for every traversal, and having to create and execute the SOAP call to validate the token.

Additional benefits of passive validation in a federated SSO system:

- Allows traversal via 'plain old HTML web links' so an RP's web applications can easily provide HTML links to other RP applications in the EE-FIM trust framework.
- Users can create standard browser bookmarks for RP applications in the EE-FIM
- Users are able to email links to RP applications.
- Users may type or cut and paste URLs for RP applications directly in their web browser.
- The EE-FIM network can grow naturally as additional RP application are added.
- 'Favorite Links' feature in an RP application will work with all RPs in the federated SSO. This was implemented and demonstrated in the EPA Portal application.

A fully functional proof of concept of this RP traversal (federated SSO), using passive validation, was implemented by NMED, WYDEQ, and NDDoH, EPA Portal, and EPA Enterprise Security Bridge teams as part of the original ISOL project. This was presented at the EN 2017 conference in Philadelphia. The slides and video of the presentation are available here and here. Note that ordinary web links, bookmarks, and direct entry of URLs (i.e. normal web usage) are all that is needed to traverse from RP to RP in different states after the initial IdP login.

Supplementary Project Documentation

The NMED research team assembled the complete EE-FIM project documentation into a repository for ease of reference. The documentation includes the project charter, status reports, discovery sessions meetings, questionnaires, implementation notes, gap analysis, recommendations, and presentations.

Appendix B - Integration Options for IdP and RP Roles

Identity Provider (IdP) Options

The ID Bridge architecture provides three options to state partners for integration in the role of an Identity Provider (IdP), thus allowing access to the trust framework via the partner's existing identity management credentials - e.g. NMED's SEP or WYDEQ's ENVITE.

The following IdP choices are available:

IdP Option X	*3rd Party Option*: Install a free, open source stand-alone Identity Provider (IdP) with focus on OpenID Connect Protocol (OIDC) in the same manner as Google's OIDC IdP. Connection to the partner's existing identity store from the chosen OIDC software may be via a protocol (i.e. Active Directory), via database, or via local web services. This allows the IdP software to create a token to send to the Bridge that includes the necessary user claims. This requires at most a few days to install and configure the software.
IdP Option Y	*Configuration-only connection* to WS-Federation Trust Framework (Microsoft IIS only) + *createTokenService()* web service via SOAP / WSDL. For this option, programming is required to build the required claims, which are retrieved from the user identity store. The difficulty level varies, depending on the type of identity store- e.g., Active Directory may take very little time, while an RDBS might take much more. This option is optimal for States and partners already using Microsoft technologies.
IdP Option Z	*Programmatic connection* to WS-Federation Trust Framework + *createTokenService()* web service via SOAP / WSDL. Significant development activities are required for this approach, which include but are not limited to: establish the connection to the bridge; user store integration; creating the claims; using the SOAP calls to Bridge for creating token. This approach involves several weeks of programming time to write software to connect to the trust framework and to utilize the SOAP web services. This option is mostly suited for States and partners who do not have sufficient flexibility regarding new technology adaptation -- e.g., if heavily reliant on legacy systems or databases

Table 1: IdP Options

Guidance for Partners - Identity Provider (IdP)

Choose standalone, technology-appropriate, well-supported open source IdP software products. Select products supporting the OpenID Connect (OIDC) Protocol, which is preferred by the

computer industry for ease of use, and for future IdP applicability to mobile apps. During the development of a federated IDM system prototype, New Mexico successfully deployed the phpOIDC IdP software using the web services as the connection to the SEP identity store. Use of the web services connection to the identity store required a few hours of custom software development. Additionally, Wyoming successfully utilized the IdentityServer IdP software using the database identity store connection, thus requiring no programming at all.

In order to establish a system as an IdP with the bridge, the following are required:

1. The IdP authentication URL - This is the URL Bridge uses to redirect the user to the IdP for authentication (from the page where the Bridge lists all of the IdP choices)
2. The security certificate used for signing the SAML token. The Bridge needs the thumbprint of the certificate in order to establish a trust relationship.
3. A temporary test account which can be used to login through IdP. The test account can be removed after successful integration.

Declined Identity Provider (IdP) Options

NMED did not choose the *Configuration-only connection* to WS-Federation Trust Framework (Microsoft IIS only), since NM does not use Microsoft IIS. NMED could have stood up separate Microsoft Windows servers and configured them to run the Microsoft IIS web server, however, this would have entailed significant costs for server hardware (or VMs) and Windows operating systems licenses, as well as the need for ongoing maintenance.

NMED chose not to use the *Programmatic connection* to WS-Federation Trust Framework + *createTokenService()* web service via SOAP / WSDL, because it would have required a significant amount of Java EE programming to modify SEP. Further, we wished to abide by the general engineering principle of *separation of concerns* so that SEP would not become a kitchen sink of IDM services. A secondary consideration is that NMED concludes that the programming overhead and complexity of the SOAP web service protocol to be needlessly burdensome. NMED has a strong architectural preference for using RESTful web services.

Relying Party (RP) Options

The EN Enterprise Security Bridge architecture provides several options to state partners for integration in the role of an Relying Party (RP), thus extending access to partner's web applications to other trust framework partners. For example, North Dakota's DoH can allow access to their ERIS application to users from NMED and WYDEQ.

The following RP choices are available:

RP Option A	"Configuration-only" connection to WS-Federation Trust Framework is very easy, but restricted to RPs using the Microsoft IIS web server. Additionally, RP will still require traversal method of Option B or Option C.

RP Option B	Active RP secure token validation and traversal, which requires specially constructed and managed 'active' HTML links or buttons. These 'active' links use HTTPS POST to invoke programmatic connection to WS-Federation Trust Framework (e.g. auth10 framework in Java) plus programmatic invocation of the Bridge's validateToken() web service via SOAP / WSDL. May be implemented in any web application language (Java EE, PHP, etc.)
RP Option C	*Recommended Option*: Passive RP secure token validation and traversal using 'plain old HTML links'. Traversal is done *without* the RP actively and explicitly passing STS Token - rather the STS is implicitly and passively authenticated via HTTPS redirect to the Bridge, which then automatically utilizes secure STS web cookies to authenticate. May be implemented in any web application language (Java EE, PHP, etc.)

Table 2: RP Options

Guidance for Partners - Relying Party (RP)

Partner RP applications should use passive validation with the Bridge. This is done by simple HTTPS redirects as documented in the updated Bridge developer's guide. This requires much less RP programming for traversal. More importantly, it removes a major burden from RPs because they do not have to create and track STS tokens and maintain extensive special 'active' links or buttons to every other RP web application in the ecosystem. Passive RP traversal provides the best user experience of a true federated SSO, allowing seamless RP traversal via standard html links and bookmarks, while having only to login a single time.

To implement WS-Federation for RP Option B, partner RPs should choose well-supported open source libraries that are appropriate for the RP web application framework. For example: Microsoft WIF (.NET built-in), Apache CXF Fediz (Java), or SimpleSAMLphp (PHP). To implement the SAML protocol that is needed for all options, partner RPs should also select technology-appropriate, well-supported open source libraries. Available libraries include: SimpleSAMLphp (PHP), OpenSAML (Java), Spring Security (Java), or WIF (.NET built-in).

The Relying Party needs to provide the following to the Bridge for the initial configuration:

1. The realm/domain URL of the RP.
2. The thumbprint of the installed security certificate to establish the trust relationship.

Declined Relying Party (RP) Options

Configuration-only connection to WS-Federation Trust Framework (Microsoft IIS only) + active validation via validateToken() web service via SOAP / WSDL. This is not a viable option for NMED because NMED uses Linux servers, Apache web servers, and Java EE web applications. It would be very expensive to add Microsoft servers with Microsoft IIS web servers just for purposes of the EE-FIM, as four sets of servers would be needed for NMED's multiple server environments: Test, Development, Integration (Quality Assurance), and Production.

P*rogrammatic connection to WS-Federation with active validation* option was declined because active validation in a FIM makes traversal across RPs difficulty and cumbersome and would require extensive additional burdens on RPs both technically and in governance.See *Appendix D*. Active validation in a FIM is not scalable because all RPs in the trust framework would require additional programming to create specially constructed HTML ‘active links’ or buttons that invoke web services. User’s could not create bookmarks for RP web applications nor email RP links. These observations are based on experience, since NMED actually implemented this approach for both Java EE and PHP, before abandoning it due to the reasons above.
Passive validation allows traversal via ‘plain old HTML web links’ so an RP’s web applications can easily link to other RP applications in the EE-FIM trust framework. Additionally, this allows users of the EE-FIM to create standard browser bookmarks for RP applications, as well as email links to RP applications.

Active validation, on the other hand, makes traversal across RPs difficult and cumbersome in an federated identity management (FIM) system. Using active validation would require extensive additional burdens on RPs both technically and in governance. With active validation, all RPs in the trust framework would require additional programming to create specially constructed HTML ‘active links’ or buttons that invoke SOAP-based web services. User’s could not create bookmarks for RP web applications nor email RP links.

Appendix C - Partner Integration Engagements

The timeline of the project followed a structured series of steps built to engage all of the partners and collect as much information as possible about their existing configuration, Partner needs, their thoughts on how a Federated Identity Management System would fit within their existing environment and all technical hurdles were explored. The sequence of these sessions was as follows:

Partner Discovery Sessions

NMED created “Discovery Questionnaires” to generate a clear understanding of the Information Technology (IT) operating environment and identity management (IDM) system of each state partner for integration to the EN Enterprise Security Bridge. The first questionnaire was a one-page summary of IT and IDM systems, while the second questionnaire contained more detailed questions and space for partners to write extended descriptions of their IT and IDM architecture and technology stack. The questionnaires were sent via email prior to in-person discovery sessions at the partner’ offices.

Each discovery session facilitated information exchange between the state partner, the NMED research team, and the EPA Bridge team. The state partner provided live demos of their EPA-related web applications and IDM systems, followed by in-depth discussions. The NMED team presented the EE FIM project overview and results of research thus far.

The EPA Bridge team joined via teleconference to present a technical overview of the EN Enterprise Security Bridge, WS-Federation trust framework, and secure token services. The concluding meetings explored what the state partner saw as potential benefits of participating in the EE-FIM, along with outlining the follow-up steps to move forward with a technical implementation.

New Mexico Environment Department

New Mexico Discovery and Analysis

NMED Technology Platform

The computer platforms and operating environment used by the New Mexico Environment Department includes servers running the Linux Red Hat operating system, Apache web server, and Tomcat Java EE web application framework. Additionally, the PHP web application framework runs some NMED and third-party web applications. All databases are implemented using Oracle Enterprise database servers. The web development programming languages used are Java (Java EE), PHP, and Oracle PL/SQL. The software development frameworks and APIs utilized include Spring Security, JBoss Seam, JSP, JSF, RichFaces (all Java), and CodeIgniter (PHP).

NMED Single Sign-on System

New Mexico uses SEP (Secure Extranet Portal) as the Identity Management System (IDM). SEP is an authentication system and web application gateway. SEP was implemented using an Oracle Database, Oracle PL/SQL stored procedures, and the Java-based Spring Security framework. SEP provides a web application portal (gateway), Identity Provider, identity store, Secure Token Service (STS), authentication system, and authorization system - all in a single framework that supports the development of web applications, web services, and API libraries. More than 25 web applications use SEP for Single Sign-On (SSO) services and identity management services, including both Java EE and PHP applications.

The SEP architecture was developed to provide a web application gateway via a Single Sign-On system for NMED web applications. The SEP system provides department-wide web application access. SEP uses Java Spring Security as the primary security framework for both authentication and authorization, which utilizes concepts from the OpenID authentication framework, together with the OAuth2 protocols and security tokens. The identity store for user accounts is a custom Oracle Database, which includes Oracle PL/SQL stored procedures for identity validation and user account services.

The design of the SEP architecture comprises registration, administration, and decentralized authorization and role management by application owners. Additionally, a SEP API was developed for validation of active sessions and access to user information. This is especially useful for integration of 3rd-party applications. SEP works as an SSO gateway to registered web applications for authenticated users. The application owner authorizes access and assigns user roles for their specific application, within the SEP SSO gateway framework.

The SEP design also provides for extending its security framework to external applications, including COTS and open source third-party applications. For in-house applications, this is implemented via the SEP_SECURITY package of Oracle stored procedures, which allow NMED web applications to use SEP's identity store database for user authentication, validation, and authorization. Additionally, there is a RESTful SEP API (written in PHP), which provides "SEP Single-Sign-On as a Service", so open source or COTS third-party applications don't have to call Oracle procedures - and thus, don't require access to the SEP Oracle database. The SEP API design allows web applications that that are *not* part of the SEP family of Java applications to be integrated within the SEP SSO system. This includes, for example, PHP applications and COTS applications. This aspect of the SEP API enhances security and ease of maintenance. It is a best practice for separation of concerns in a microservices architecture.

NMED Discovery Session

The NMED EE-FIM research team met with the NMED software engineers and managers responsible for the Secure Extranet Portal (SEP). The SEP team provided live demos of their IDM system, Single Sign-On (SSO) system, and EPA-related web applications. This was followed by in-depth discussions of NMED's identity systems and the EE-FIM integration options. The NMED research team presented the EE-FIM project overview and results of research thus far. The EPA Enterprise Security Bridge team joined via teleconference to present a technical overview of the Bridge, WS-Federation trust framework, and Secure Token Services (STS).

SEP account creation is is handled by a fully automated via web signup form, which employs a confirmation email. Each SEP web application has a designated administrator to authorize access and assign roles and permissions for each user account.

Identified Strengths of the SEP IDM:

- Single Sign-On (SSO) web application gateway that makes user's work easier
- Wide adoption for both in-house applications and external 3rd-party apps
- Proven, battle-tested, and mature system
- Developed using industry-standard technologies: Java EE, Spring, and Oracle
- Simple administration
- Wholly-owned by NMED and deployed on NMED servers
- Self-service administration including user sign-up, confirmation, account creation, and maintenance such as a password reset feature
- Local individualized administration for each web application
- RESTful SEP API provides "SEP Single-Sign-On as a Service" so external and third party web apps can be integrated with the SEP SSO system.

Identified Weaknesses of the SEP system:

- Custom made application
- Locally stored passwords (Oracle)

- Does not currently support multi-factor authentication
- Outdated version of Spring Security (soon to be updated)
- No auto-redirect when re-authenticating
- Can't modify timeouts on a per-app basis
- Users can be confused by "back-end" timeout (sessions are valid for 2 hours only)
- SEP database schema access can be slow due to architectural decisions

The concluding meetings explored what NMED's SEP team saw as potential benefits of participating in the EE-FIM, along with outlining the follow-up steps to move forward with a technical implementation. The benefits mentioned by NMED were the ability to expand the SEP user base without increasing maintenance, as well as improved ease-of-use for users working with multiple agencies or multiple states via federated single sign-on (SSO).

The in-depth discussions centered on the Discovery Questionnaires prepared by the NMED research team. The first questionnaire (see table below) is a one-page summary of IT and IDM systems, while the second questionnaire (link below) contains more detailed and open-ended questions about IT and IDM architecture and technology stack, as well as potential integration with the EE-FIM system. Below is the link to the discovery questionnaire, followed by the discovery session summary.

NMED Discovery Questionnaire

NMED – Identity Management (IDM) System and Single Sign-On (SSO) System	
Identity Store	Oracle Database for SSO. There are 25+ web applications using SEP for Identity Management. Also Active Directory (AD) and MS Exchange
Identity Framework	Java Spring Security
Identity SSO Server/Bridge	Secure Extranet Portal (SEP) - uses Java Spring Security - developed in house via contractor.
Identity SSO Protocols	OAuth2
Identity SSO Tokens	OAuth2
Secure SSO Token Service	Java Spring Security
SSO Portal and SSO Identity Provider (IdP)	Secure Extranet Portal (SEP) provides a Portal, Identity Provider, and Secure Token Service all in one application. There are 25+ web applications using SEP for SSO - mix of Java and PHP.
SSO Database	Oracle (PL/SQL) - SEP uses a custom built database.
Identity SSO Authorization	Authorization uses roles stored in the database. Typically: User, App Admin, and SEP Admin. Some apps have app-specific roles (e.g. SQUID). App owner authorizes access and assigns user roles for their app.

Identity SSO Claims	user id, email, first name, last name, middle initial, title, street 1, city, state, zip, phone, fax, street 2, creation date, is cromerr registered, roles, is activated, created by, modified by, modified date, org, dept, employment type, is nmed employee, password date
.NET Relying Party (RP)	n/a
Java Relying Party (RP)	Java - Spring Security
Relying Party (RP) API	Java - Spring Security | PHP - RESTful web services
SharePoint Integration	n/a
Operating System	Linux - Red Hat Enterprise Linux Server release
Web Server	Apache HTTP Server
Web App Framework	Apache Tomcat - Java EE Server
Web App Language	Java EE, PHP - Spring, JBoss Seam, JSP, JSF, RichFaces, CodeIgniter
Database Server	Oracle 11g Enterprise Edition Release
Document Server	None - Documents stored as BLOB datatype in Oracle database.
Firewalls	Application-layer firewalls for internal/external users. Ports 80, 443 open.

Table 3: NMED Discovery Session Summary

New Mexico Integration Solution

The NMED EE-FIM research team worked with software engineers responsible for NMED's SEP IDM system to integrate the SEP web application gateway into the EN Enterprise Security Bridge. The process was driven by NMED's existing IT operating environment, web application frameworks, and database technologies. For NMED, these are Linux OS, Apache web server, Tomcat Java EE web application framework, Spring Security, and Oracle database. Once the technical approach was agreed upon, work began to integrate SEP with the Bridge. The software engineers from the Bridge team provided technical expertise for testing and debugging the implementation. They also registered NMED's web servers and application endpoint URLs with the Bridge, as well as handling an exchanging of keys between the Bridge and SEP (acting as a relying party - RP) and to NMED's phpOP identity provider (IdP). NMED chose to implement a phpOP identity provider solution because it integrated well with the existing architecture, necessitated the smallest number and scale of changes to NMED's existing SEP system, and NMED integration staff were most familiar and comfortable with this technology.

The relying party (RP) implementation (more detail below) was done first because it is the more fundamental and useful way to participate in the EE-FIM trust framework. Another reason for this was that the Bridge Team had already implemented several identity providers (IdP) before the EE-FIM project began. Thus, each state partner could use the existing Exchange Network IdP for testing, as well as public IdPs such as Facebook and Google.

Integration Choices

NMED chose to participate in both EE-FIM roles: Identity Provider (IdP) and Relying Party (RP). The integration options chosen are shown in the table below. Refer to *Appendix B - Integration Options for IdP and RP Roles* for further technical details.

Identity Provider (IdP)	NMED chose to implement a stand-alone Identity Provider (IdP) using the OpenID Connect (OIDC) protocol, in the same manner as Google's OIDC IdP.
Relying Party (RP)	NMED chose to implement the WS-Federation Passive Requestor Profile (provided by the EN Enterprise Security Bridge) for passive secure token validation and traversal.

Table 4: NMED Integration Choices

Identity Provider (IdP) Integration

NMED chose to integrate a stand-alone Identity Provider (IdP) using the OpenID Connect (OIDC) protocol, in the same manner as Google's OIDC IdP. The primary reason for this choice was our analysis that it would be easiest and fastest approach, as it would require either very little or no programming work. Also, there were several free, open source IdPs available for many web frameworks, including Java EE, .NET, and PHP. NMED also wanted to use the latest technology that aligns with major companies such as Google. Additionally, OIDC was clearly the newest and most widely adopted of the IdP technologies. The stand-alone IdP approach would also allow the NMENV IdP to be used in other future IDM applications in contexts completely separate from the EPA-developed EN Enterprise Security Bridge. Finally, this choice would involve the lightest touch on existing systems. In fact, this approach did not require any changes at all to SEP.

Our analysis concluded that a stand-alone IdP would require either no programming or only minimal programming to connect to the identity store database. This analysis proved to be true. A direct connection to the identity store - i.e. the SEP Oracle database - would have required no programming work. However, to enhance security and provide a more robust solution and because SEP doesn't support one of the EN Enterprise Security Bridge's accepted protocols, we chose to connect to our SEP Oracle database via our SEP API RESTful web service. This required a small amount of programming modification to the open-source phpOIDC IdP application.

IdP Integration Difficulty Level and Implementation Time

Medium-Low / 2-3 Weeks - OpenID Connect (OIDC) Stand-Alone Server
NMED used the open source phpOIDC server applications and API library to install and configure an IdP server. Out of the box - the OIDC protocols used by the phpOP IdP server application result in the server generating a JWT authentication token when a user logs in. This

JWT token is then posted to the Bridge, where the Bridge's Multi-Protocol IdP Manager decrypts the JWT identity claims and passes them to the Secure Token Services (STS) subsystem. The STS then translates these identity claims into a shared common STS token format (as part of a SAML assertion), which is used throughout the EE-FIM trust framework.

Relying Party (RP) Integration

NMED chose the WS-Federation Passive Requestor Profile (provided by the EN Enterprise Security Bridge) for passive secure token validation and traversal. The Bridge implements the WS-Federation protocols and profiles, which specifically provides a passive validation mechanism for client systems that don't have an active SOAP-based mechanism available – i.e. web browsers, which are so widely used to access web applications. For technical details, please refer to the linked articles below.

> *Understanding WS-Federation — Passive Requestor Profile*
>
> Understanding WS-Federation

NMED implemented this passive RP validation for *both* it's Java EE-based SEP portal, as well as a PHP test web application using the phpRP component of phpOIDC (simply for learning and exploratory purposes - it was not part of the final implementation). To connect to the Bridge's via the WS-Federation trust framework via Java, we used the auth10 library. For the PHP test application, the WS-Federation connection used the simpleSAMLphp library.

For the SAML token processing in Java EE, SEP utilized the OpenSAML library. For SAML token processing in the PHP test application, NMED used the simpleSAMLphp library (which also supports WS-Federation - see above). There are many free SAML libraries available for all major web application languages: http://saml.xml.org/wiki/saml-open-source-implementations.

RP Integration Difficulty Level and Implementation Time

High / 4 weeks - *WS-Federation Passive Requestor Profile for passive secure token validation and traversal*

Integrating with the EN Enterprise Security Bridge took almost 4 weeks since NMED's SEP uses an entirely different technology stack compared with the Bridge. The Bridge is based on Microsoft Windows, IIS, WIF, and .NET framework, while NMED's SEP is implemented on Linux, Apache, and Java EE framework. For the Java EE-based SEP, the external library *auth10* was used to connect with the WS-Federation trust framework. The *OpenSAML* library was used to parse the SAML assertion returned by the Bridge.

Identity Provider and Relying Party Integration Steps

The steps can be found in the NM Integration Worksheet

Recommended tools, frameworks, web resources

IdP - phpOIDC (PHP) or MITERid Connect (Java) or Gluu Server (Java)
RP - auth10 and OpenSAML (Java) or simpleSAMLPHP (PHP)

Wyoming Department of Environmental Quality

Wyoming Discovery and Analysis

WDEQ Technology Platform

The computer platforms and operating environment used by the Wyoming Department of Environment Quality (WDEQ) includes servers running the Microsoft Windows Server operating system, Microsoft IIS web server, and Microsoft .NET web application framework. Additionally, the Java EE web application framework runs some WDEQ and third-party web applications. All databases are implemented using Microsoft SQL Server database servers. The web application development programming languages used are C# .NET, Java (Java EE), and T-SQL. The software development frameworks and APIs utilized include Microsoft .NET Framework, Windows Identity Foundation (WIF), ThinkTecture Identity Server, ASP .NET and SharePoint.

WDEQ Identity Management System (IDM)

Statewide IDM, eGov, is used by WDEQ for Identity Management. WDEQ also implemented a more secure IDM layer called ENV-ITE or ENVITE (Environment IT Environment). Additionally, ENVITE implements CROMERR compliant reporting. eGov is a user management system provided to the Wyoming Dept. of Environmental Quality (DEQ) by the State of Wyoming Enterprise Technology Services (ETS). eGov includes an identity management (IDM) system that uses Microsoft SQL Server for its identity store. ENVITE implements a web gateway single sign-on (SSO) system for WDEQ's industry partners (regulated community). Internal staff use database applications that do not provide an SSO.

The eGov IDM is administered and governed by their central IT group, ETS. Anyone with internet access can obtain an eGov account via the statewide portal. Once that is obtained, if a user wishes to utilize WDEQ applications, they use the ENVITE system with their eGov credentials to request access. Identity proofing for access to WDEQ applications is done in the ENVITE system and via a process including a notarized affidavit. No identity proofing is done in the eGov IDM system. The eGov IDM security system uses username and password for authentication. ENVITE uses username, password, pin, and secret questions in order to comply with the EPA's CROMERR security policies.

The IDM for WDEQ uses eGov / ENVITE for industry partners and Active Directory for internal staff members. Also, all WDEQ staff receive a Google ID to access Google Apps. For ENVITE access, the scanned affidavit must be from an original document (all completed documents require an ink signature). It cannot be a document that is scanned and emailed.

WDEQ Discovery Session

The NMED EE-FIM research team traveled to Cheyenne Wyoming to meet with the WDEQ software engineers and managers responsible for the ENVITE portal and web gateway system. The WDEQ team provided live demos of their IDM system, single sign-on (SSO) system, and EPA-related web applications. This was followed by in-depth discussions of WDEQ's identity management systems and the EE-FIM integration options.

The NMED research team presented the EE-FIM project overview and results of their research thus far. The EPA Enterprise Security Bridge team also joined the discussion via teleconference to present a technical overview of the EN Enterprise Security Bridge, WS-Federation trust framework, and Secure Token Services (STS).

Identified Strengths of current eGov / ENVITE IDM system:

- CROMERR-compliant system implemented within ENVITE
- Flexible to many systems and coding environments (e.g. .NET, Java EE, PHP)
- Successful operation of IDM systems for three years.
- Single Sign-On (SSO) web application gateway that simplifies user's work
- Used by both in-house applications and external 3rd-party apps
- Developed using industry-standard technologies: .NET, WS-Federation, and WIF
- Simple, straight-forward administration

Identified Weaknesses of the eGov / ENVITE IDM system:

- Custom made application
- Inability to change or find your login ID without your SSN or calling ETS for support (this is called self-service in the IDM industry)
- Does not currently support multi-factor authentication
- Difficulty training industry partners how to complete the ENVITE (CROMEER) application process. Since WDEQ began using ENVITE, they have had to modify their instructions, screens, and affidavits to help the partners be more successful in achieving their account sign-on credentials in a timely manner
- Procuring funding to implement appropriate systems and modifications

The concluding meetings explored what WDEQ's ENVITE team saw as potential benefits of participating in the EE-FIM, along with outlining the follow-up steps to move forward with a technical implementation. The benefits of participating were identified by WDEQ as simplification of the process for industry partners (i.e. use of the same username and password for multiple systems) and decreased technical management by WDEQ IT staff.

WDEQ expressed a major concern that using a federated IDM system from outside the state of Wyoming would necessitate a high level of coordination for any changes to the system that might necessitate changes in the ENVITE system or other permitting applications. The concern was focused primarily as relating to the arrangement of funding for any necessary development

effort. Challenges in deploying the EE-FIM system included acquiring funding for development, and outreach to industry partners. WDEQ would need adequate time to ensure funding is in place, and training materials and opportunities would need to be established to ease any transitions for industry partners and staff.

Other ideas regarding the EE-FIM system were also discussed. A company conducting business in multiple states could “share” identity affidavit for permits. A sensible policy on password changes would be needed, since some users use WDEQ applications irregularly (i.e. annually). Thus, a forced change of password every 90 days would not work well for users in this scenario.

Additionally, WDEQ personnel believe that a policy of trust between partners needs to be established in order to become an IdP. A minimum standard that must be enforced could help firm up that trust. There is also a clear need to organize a board of members to make decisions, perhaps with technology hosted by a 3rd-party through a subscription model. It goes against an organization’s nature to give up control to trust other sources but they believe that this needs to happen in order for the EE-FIM trust framework to be a success. The university research consortium (Shibboleth) federated trust framework example is a great example of how this type of trust can be successfully managed.

Related to the issue of trust between organizations or governing bodies, there are significant adoption issues that WDEQ feels will be challenging to overcome. They feel that the industry is screaming for simplicity and standardization so can we learn from other communities on how collaboration has been successful? They referenced Department of Transportation truck driving certificates which are recognized and honored across state border lines This does not have to be an all-or-nothing approach - starting out with a small group and then using a push from industry to move into other states would likely be most beneficial.

The in-depth discussions during the visit centered on the Discovery Questionnaires initially prepared by the NMED research team. The first questionnaire (see table below) is a one-page summary of IT and IDM systems, while the second questionnaire (link below) contains more detailed and open-ended questions about IT and IDM architecture and the technology stack, as well as potential integration with the EE-FIM system. Below is the link to the discovery questionnaire, followed by the discovery session summary.

WDEQ Discovery Questionnaire

WDEQ – Identity Management (IDM) System and Single Sign-On (SSO) System	
Microsoft Windows .NET Environment	
Identity Store	Microsoft SQL Server database – statewide via: state eGov profile – https://egov.state.wy.us. More than 50 Wyoming state websites use eGov

	for their IDM.
Identity Framework	WS-Federation and WS-Trust via Microsoft Windows Identity Foundation (WIF) API – version WIF 4.5
Identity SSO Server/Bridge	Thinktecture Identity Server v2 – based on: NET 4.5, MVC 4, Web API, and WCF
Identity SSO Protocols	WS-Trust, WS-Federation, OAuth2, HTTPS GET
Identity SSO Tokens	SAML 1.1/2.0, JSON Web Tokens (JWT) [JWT used by OpenID Connect]
Secure SSO Token Service	WIF 4.5
SSO Portal and SSO Identity Provider (IdP)	ENVITE provides a Portal, Identity Provider, and Secure Token Service all in one application (solution). ENV-ITE currently allows access request for 4 web apps: eDMR (Water Quality), IMPACT (Air Quality), and MIDAS (Land Quality) and WYPermit (COTS product from Windsor)
SSO Database	Microsoft SQL (T-SQL) – ENV-ITE utilizes an extensive, custom-built database with 100+ tables in 4 schemas: audit, dbo, idp, and reference.
Identity SSO Auth.	ASP .NET membership, roles and profile.
Identity SSO Claims	name, emailaddress, givenname, surname, role, enviteroles, application
.NET Relying Party (RP)	Integration via .NET web.config file configuration via ASP .NET FedUtil
Java Relying Party (RP)	Integration using Apache CXF Fediz API – used by WDEQ's IMPACT web app for Air Quality.
Relying Party (RP) API	RESTful Web Services – Input: HTTPS POST, Output: JSON
SharePoint Integration	SharePoint 2010 Claims Authentication Integration
Operating System	Windows Server 2008 R2 Datacenter x64
Web Server	IIS 7.5
Web App Framework	.NET Framework 4.5
Web App Language	C# .NET
Database Server	Microsoft SQL Server 2008 R2
Document Server	SharePoint 2010
Firewalls	Application-layer firewalls for internal/external users. Ports 80, 443 open.

Table 5: WDEQ Discovery Session Summary

Wyoming Integration Solution

The WDEQ's software engineers worked with the NMED EE-FIM team to integrate the ENVITE web application gateway with the EN Enterprise Security Bridge. The process was driven by WDEQ's existing IT operating environment, web application frameworks, and database technologies. For WDEQ, these are Microsoft Windows Server OS, Microsoft IIS web server, .NET C# web application framework, Microsoft WIF security and Microsoft SQL Server database. Once the technical approach was agreed upon, work began to integrate ENVITE with the Bridge. The software engineers from the EPA Enterprise Security Bridge team provided technical expertise for testing and debugging the implementation. They provide basic services also such as registering WDEQ's web servers and application endpoint URLs with the Bridge, as well as handling an exchanging of keys between the Bridge and ENVITE (acting as a relying party - RP) and also with the ENVITE identity provider (IdP).

Integration Choices

WDEQ chose to participate in both EE-FIM roles: Identity Provider (IdP) and Relying Party (RP). The integration options chosen are shown in the table below. Refer to *Appendix B - Integration Options for IdP and RP Roles* for further technical details.

Identity Provider (IdP)	WDEQ chose to implement a stand-alone Identity Provider (IdP) using the OpenID Connect (OIDC) protocol, in the same manner as Google's OIDC IdP.
Relying Party (RP)	WDEQ chose to implement the WS-Federation Passive Requestor Profile (provided by the EN Enterprise Security Bridge) for passive secure token validation and traversal.

Table 6: WDEQ Integration Choices

The relying party (RP) implementation was completed first because it is the more fundamental and useful way to participate in the EE-FIM trust framework. Another reason for this was that the EPA Enterprise Security Bridge Team had already implemented several identity providers (IdP) before the EE-FIM project began and came to this implementation with that previous experience. Thus, each state partner could use the existing Exchange Network IdP for testing, as well as public IdPs such as Facebook and Google.

Identity Provider (IdP) Integration

WDEQ chose to integrate a stand-alone Identity Provider (IdP) using the OpenID Connect (OIDC) protocol, in the same manner as Google's OIDC IdP. The primary reason for this choice was our analysis that it would be the easiest and fastest approach, as it would require either very little or no programming work. WDEQ also wanted to use the latest technology that aligns with major companies such as Google. Additionally, OIDC was clearly the newest and most

widely adopted of the IdP technologies. The stand-alone IdP approach would also allow the WDEQ IdP to be used in other future IDM applications in contexts completely separate from the EN Enterprise Security Bridge. Finally, this choice would involve the lightest touch on existing systems. In fact, this approach did not require any changes at all to their ENVITE system.

Our analysis concluded that a stand-alone IdP would require either no or only minimal programming to connect to the identity store database and this proved to be the case. Since the ENVITE system was based on the Thinktecture Identity Server, it actually already contained an identity provider (IdP) subsystem. All that was needed was to configure it to connect with the Bridge.

IdP Integration Difficulty Level and Implementation Time

Low / 1 week, WS Federation, using configuration only approach, with minimal amount of coding for sending the claims back to the Bridge.

Relying Party (RP) Integration

WDEQ chose the WS-Federation Passive Requestor Profile (provided by the EN Enterprise Security Bridge) for passive secure token validation and traversal. The Bridge implements the WS-Federation protocols and profiles, which specifically provides a passive validation mechanism for client systems that don't have an active SOAP-based mechanism available – i.e. web browsers, which are so widely used to access web applications.

WDEQ implemented this passive RP validation in the following manner. They connected to the Bridge's WS-Federation trust framework via configuration only, since ENVITE uses the Microsoft IIS web server. For the SAML token processing ENVITE utilized the Microsoft WIF library. There are many free SAML libraries available for all major web application languages: http://saml.xml.org/wiki/saml-open-source-implementations.

RP Integration Difficulty Level and Implementation Time

Medium / 2 weeks, since WDEQ is also using the same Microsoft technologies as the EN Enterprise Security Bridge, including .NET and WIF frameworks, IIS web server, and WS-Federation protocol, the integration was much less complex than for NMED, which used the Java EE technology stack.

WDEQ only had to do some straightforward configuration changes in order to connect to the Bridge via the WS-Federation protocol, as well as to receive and parse the SAML assertions containing the identity claims. This is because these Microsoft IDM systems can talk to each other without any additional coding or third party libraries. The only programming needed was to connect the federated user to a local user identity in the ENVITE system.

Identity Provider and Relying Party Integration Steps

The steps can be found in the WY Integration Worksheet

Recommended tools, frameworks, web resources

For Microsoft-based systems like WDEQ's ENVITE web application gateway, the recommended frameworks include: Microsoft Windows Identity Foundation (WIF) API library (which is now part of Windows OS), the Thinktecture Identity Server framework, and Microsoft IIS web server.

North Dakota Department of Health

North Dakota Discovery and Analysis

NDDOH Technology Platform

The computer platforms and operating environment used by the North Dakota Department of Health (NDDoH) includes servers running the Microsoft Windows Server operating system, Microsoft IIS web server, Apache 2.4 web server, and Microsoft .NET web application framework. Additionally, some NDDoH web applications require VB.NET or Microsoft Access. All databases are implemented using Microsoft SQL Server database servers. The web application development programming languages used are .NET and VB.NET, and Microsoft Access. The software development frameworks and APIs utilized include Microsoft .NET Framework, IBM Tivoli via LDAP and VB.NET.

NDDoH Identity Management System (IDM)

North Dakota utilizes two IdM Systems. Industry users and the public log into ERIS (Electronic Reporting Information System) using the *ND State login*. Internal ND state Health Department staff login to ERIS using their Active Directory, NDGOV, state account credentials. Once the login process is complete, both systems pass the user credentials to the state's ERIS system. Once the user's state account is verified, both systems pass the user credentials into ERIS where the user name is associated with the facility and reports they are authorized to submit in ERIS, for industry & public users, or with the admin role if NDDoH staff.

The ND state login system, which also leverages LDAP, uses IBM Tivoli Directory Server under the hood to provide SSO to external users. This system is known as Secureway. Both systems are managed, and their usage governed, by ND ITD.

The ND state Account which is used for sign-on to access the ERIS system is an Enterprise shared authentication services, as it is the same system used by many ND state agencies for applications that allow the public to access different services. This is a shared authentication service but it does not provide true Single-Sign-On capability across all of NDDoH's applications.

All ND staff are given the Secureway Admin role. Without it they cannot gain access ERIS. Staff Users are "setup" with Facility, "Dataflow" - the specific report type -- and Role. Each ND staffer only works on one "combo" of Facility and Dataflow at one time.

North Dakota employs ERIS for the Identity Management System. Authentication is done using an ND state account (implemented as above via LDAP), then it is passed to ERIS where the username is associated with the facility and reports they are authorized to submit in ERIS. ERIS

natively handles CROMERR compliance.

Users requesting access to ERIS must have their paper applications reviewed by program staff, and requires a subscriber agreement with a signature from the responsible official. EHS program staff must review each user application for access and determine if they can be set up. If necessary they will contact the facility and verify that the user request is authentic.

NDDoH Discovery Session

The NMED EE-FIM research team traveled to Bismarck, North Dakota to met with the NDDoH personnel who use and administer their ERIS application, as well as the ND ITD developers and managers behind North Dakota's IDM system. The ND teams provided live demos of their IDM system and ERIS. This was followed by in-depth discussions of how NDDoH identity management system works, and their options for EE-FIM integration .

The NMED research team presented the EE-FIM project overview and results of their research thus far. The EPA Enterprise Security Bridge team also joined the discussion via teleconference to present a technical overview of the EN Enterprise Security Bridge, WS-Federation trust framework, and Secure Token Services (STS).

Identified Strengths of current NDDoH IDM system:

- ND state Account is simple and efficient in that it allows users to use the same login credentials for accessing multiple state government applications.
- ND state Account has a fairly robust system to handle forgotten passwords and usernames where it will send them an email with a link to reset passwords or to get user names. This requires little human assistance which minimizes calls for help.
- Since the ND state Account system handles all of the user credentials, the Department of Health does not have the liability of storing and managing passwords.

Identified Weaknesses of the NDDoH IDM system:

- Often users do not fully understand the separation between the ND state Account login and the ERIS system for reporting, so they do at times call the Department if they lose their password or cannot login.
- Some users are confused when signing up, as they do not realize they need to setup a state account before they can submit a subscriber agreement to access the ERIS system.

The meetings included discussion of what NDDoH saw as the potential benefits and risks of participating in the EE-FIM network. NDDoH indicated that, while they have no specific plans in place, they would like to move to an electronic authentication process so they could eliminate the paper subscriber agreements currently necessary for access to ERIS. If such a move could be done as part of a larger effort to migrate to a federated ID system, they see that as a potential benefit for the larger regulated entities that have facilities in multiple states.

Some of the other potential benefits of participating in the EE-FIM network were identified during the discussion, including a greater amount of available information on permitted facilities; the potential inclusion of geolocational UX improvements, such as ‘facilities near me’; greater ease of access to public information and data submission portals; faster turnaround for new user provisioning if they could replace their current, manual Identity Proofing process; the ability to compare data submitted by a given entity to multiple states and the EPA; A Single-Sign-On capability to other NDDoH applications, such as SDWIS, Air Quality NPDS, and others; improved usability; improved access to more recent & accurate state (as opposed to Federal) data; improved ability to make data publically available; the ability to provide a means for automating requests for access to records; the potential to create data portals that combine Federal and state data; and the ability to check other states for ‘problem’ users in the regulated community.

The North Dakota teams felt that the primary benefit of EE-FIM would go to larger regulated entities who must report to multiple states, as an SSO allowing them access to all the locations to which they must submit data would vastly streamline their reporting process. Another possible benefit that was intriguing to the ND teams was the concept of a Federated Identity system providing some form of electronic authentication and/or better user and credential management tools.

North Dakota did not display a large amount of interest in extending access to users via Facebook or other Social Media IdPs on the EE-FIM network. Their opinion was that their regulated community was not a demographic that represented heavy users of social media platforms, specifically for business use. A further concern was that this might invite regulated community users to begin to mix personal and work accounts for the sake of easy login. However ND indicated that they would be open to extending such access if a compelling case were made for its benefit.

A further suggestion from ND for the EE-FIM system was to have a means to uniquely identify Facilities subject to regulation; this would streamline the process of granting access to facilities across jurisdictional boundaries.

Many of ND’s concerns and hesitation about participating in the EE-FIM network stemmed from the problems inherent in granting access to users without either a robust means of unique identification of both individual doing the reporting and the facility being reported on. ND would require a high level of trust before they would accept user authorization provided by entities other than themselves. They did indicate that were EPA and/or other state partners given the ability to reset/revoke user credentials on the EE-FIM network, that would allay much of their concern.

Much of the discussion during the visit centered on the Discovery Questionnaires initially prepared by the NMED research team. The first questionnaire (see table below) is a one-page

summary of IT and IDM systems, while the second questionnaire (link below) contains more detailed and open-ended questions about IT and IDM architecture and the technology stack, as well as potential integration with the EE-FIM system. Below is the link to the discovery questionnaire, followed by the discovery session summary.

NDDoH Discovery Questionnaire

NDDoH – Identity Management (IDM) System and Single Sign-On (SSO) System *(if applicable)*	
Microsoft Windows .NET Environment	
Identity Store	Microsoft SQL Server database – statewide via: state ND Login profile. https://apps.nd.gov/itd/ldap/login.htm. Used by over 100 ND state web apps.
Identity Framework	ND Login system's IDM is IBM Tivoli via LDAP. State Employees' IDM is Active Directory (AD)
Identity SSO Server/Bridge	n/a
Identity SSO Protocols	n/a
Identity SSO Tokens	n/a
Secure SSO Token Service	n/a
SSO Portal and SSO Identity Provider (IdP)	n/a
IDM Database	Microsoft SQL (T-SQL) – ERIS utilizes an extensive, custom-built database.
IDM Authorization	ERIS account, roles (Read Only, Add, Submit, Admin) and profile.
IDM Claims	Login name, First name, Last name, Email address, Title, Phone, Phone ext, Fax number, PIN hash, Directory type, Last Login, Date, Start date, End date
.NET Relying Party (RP)	Integration via .NET web.config file configuration via ASP .NET FedUtil

Java Relying Party (RP)	n/a
Relying Party (RP) API	RESTful Web Services for both LDAP & AD– Input: HTTPS POST, Output: JSON
SharePoint Integration	n/a
Operating System	Windows Server 2008 R2 Datacenter x64
Web Server	IIS 7.5 and also Apache 2.4 w/Mod Proxy
Web App Framework	.NET Framework 4.5
Web App Language	VB .NET for ERIS Web App. MS Access for UI for ERIS Admin Functions.
Database Server	Microsoft SQL Server 2012
Document Server	ERIS (docs stored on SQL Server) - PDF and dynamically generated PDF
Firewalls	Application-layer firewalls for internal and external users. Ports 80 and 443 open.

Table 7: NDDoH Discovery Session Summary

North Dakota Integration Solution

NDDoH and the ND centralized IT department worked with the NM EE-FIM team to integrate their ERIS system onto the Bridge as both an RP and IDP. ERIS authentication is implemented via LDAP, supported by IBM Tivoli Directory Server under the hood for external users, and via ND's state Active Directory (NDGOV) for state employees. Their technology stack was based on .NET and the VB.net framework. So, overall, the integration with the Bridge was fairly easy for North Dakota. The software engineers from the EPA Enterprise Security Bridge team provided technical expertise for testing and debugging the implementation. They also provided basic services such as registering NDDoH's web servers and application endpoint URLs with the Bridge, as well as handling an exchange of keys ("thumbprints") between the Bridge and ERIS -- acting as a relying party (RP), as well as an identity provider (IdP).

Integration Options

NDDoH chose to participate in both EE-FIM roles: Identity Provider (IdP) and Relying Party (RP). The integration options chosen are shown in the table below. Refer to *Appendix B* - *Integration Options for IdP and RP Roles* for further technical details.

Identity Provider (IdP)	ERIS utilizes IBM Tivoli via LDAP for external users, and Active Directory for State Employees as their internal Identity Management.Configuring ERIS as

	an IDP with the Bridge was done using the configuration only approach, with minimal amount of coding to configure and send the claims back to the EPA bridge.
Relying Party (RP)	NDDoH chose to implement the WS-Federation Passive Requestor Profile (provided by the EN Enterprise Security Bridge) for passive secure token validation and traversal.

Table 8: NDDoH Integration Choices

Like WY, the relying party (RP) implementation was completed initially because it was the more straightforward to implement and the most useful way to participate in the EE-FIM trust framework. They were also able to leverage the work that the EE-FIM project team had done for the RP role prior to this implementation.

Identity Provider (IdP) Integration

ND-ITD held discussions with the EE-FIM team regarding the implementation of a stand-alone Identity Provider (IdP), perhaps via leveraging the Thinktecture Identity Server as did Wyoming.

The steps for IdP implementation can be found in the gap analysis document.

IdP Integration Difficulty Level and Implementation Time

Medium / 2 weeks; leveraging WS Federation, using the configuration only approach, with a minimal amount of coding for configuring and sending the claims back to Bridge.
Note: The difficulty level listed as medium, despite ease of implementation, since NDDoH development resources were not easily available

Relying Party (RP) Integration

North Dakota also chose the WS-Federation Passive Requestor Profile (provided by the EN Enterprise Security Bridge) for passive secure token validation and traversal, similar to what Wyoming had done. As with Wyoming's RP implementation, the Bridge implements the WS-Federation protocols and profiles, which specifically provides a passive validation mechanism for client systems, such as browsers, that don't have an active SOAP-based mechanism.

NDDoH/ND-ITD implemented the passive RP validation in the same manner proven effective by Wyoming, using the configuration only approach to leverage the WS-Federation trust framework to connect to the EPA-developed EN Enterprise Security Bridge. This allowed use of the *createTokenService()* web service via SOAP / WSDL. Again similar to Wyoming, and since ND also uses the Microsoft IIS web server, ND leveraged the Microsoft WIF library for SAML token processing, vastly reducing the amount of code needed for SAML parsing.

RP Integration Difficulty Level and Implementation Time

Medium / 2 weeks, since ND also was using the same Microsoft technologies as WDEQ and the Bridge, the integration was much less complex than for NMED, which used the Java EE technology stack. As with WY, these technologies include .NET and WIF frameworks, IIS web server, and the WS-Federation protocol, all of which were leverage-able by ND with only a small number of changes to their configurations.

Identity Provider and Relying Party Integration Steps

The steps can be found in the ND Integration Worksheet

Recommended tools, frameworks, web resources

As with WDEQ, for Microsoft-based systems like North Dakota, the recommended frameworks include: Microsoft Windows Identity Foundation (WIF) API library (now part of Windows OS), the Thinktecture Identity Server framework, and Microsoft IIS web server.

Appendix D - Traversal Whitepaper sent to EPA OEI on 2/12/17

The E-Enterprise Integrated Solutions (ISOL) Project

EPA Identity Bridge - Proposal for Federated Single Sign-On (SSO)

Overview

The ability for users to traverse smoothly from one Relying Party (RP) to another without needing to re-authenticate is an expected and desirable function of a Federated Identity Management (IdM) system. The E-Enterprise Shared Identity Management Concept of Operations (ConOps) identifies a "seamless user experience between partner systems and services" as one of the "primary benefits" of such a system.[4] The EPA's Identity (ID) Bridge system was designed to meet the requirements laid out in the ConOps, and currently employs a method of RP traversal in which RPs create 'active' links[5] that post Secure Token Services (STS) Tokens to other RPs. The RP that receives an STS Token then invokes the Bridge web service method validateToken(). Although this allows smooth traversal, it both requires significant work for partner RPs to implement and maintain these links and necessitates that users modify their online navigation habits to utilize them.

We propose that the ID Bridge component of the Federated IdM system leverage the Microsoft Windows Identity Foundation (WIF) features that provide for Federated Single Sign-On (SSO) via session cookies (a 'passive' link[6] method)[7] in order to reduce the burden on partner RPs and allow users to experience the benefits of this Federated IdM system without changing their behavior. Since WIF is already the underlying technology used by the ID Bridge, implementing these features should be relatively straightforward,[8] and will provide significant benefits, including:

---

[4] "E-Enterprise Shared Identity Concept of Operations," June 24, 2016, 7-8. The ConOps also specifically requires SSO across partner web applications (17) and states that the tokens generated after the first authentication should "provide proof of authentication to any subsequent actions within E-Enterprise" (34).
[5] An 'active' link is a dynamic, programmatically generated link that transmits an STS token through an HTTP Post via JavaScript or HTML form.
[6] A 'passive' link is a standard, static HTML link or URL.
[7] This is also referred to as 'passive federation.' Michèle Leroux Bustamante, "A Crash-Course in Windows Identity Federation," *Dev Pro*, December 2, 2009, http://devproconnections.com/net-framework/crash-course-windows-identity-foundation.
[8] In fact, the current design of the ID Bridge is already creating and depositing session cookies (NMED has verified this through testing).

- increasing the **usability** of the system by reducing the number of times users must authenticate and allowing traversal of RP applications via standard HTML links and bookmarks;
- reducing the burden of **implementation** for partner RPs by eliminating the need to create and maintain extensive lists of links and firewall rules;
- encouraging widespread **adoption** of this IdM system by providing a more end-user friendly and easily implemented path to participation, as well as by aligning with underlying Microsoft WIF technologies; and
- meeting system **security** needs by employing standard methodologies used throughout the industry and ameliorating some risks posed by the current system.

Usability

Users expect that a Federated SSO (like any other SSO) will allow them to sign-in a single time and then be able to traverse to any other application or website in the ecosystem of federated trust without re-authenticating. The current ID Bridge system only allows this functionality through the use of specially constructed 'active' links by each RP, which requires users to select those special links on each partner's RP sites to navigate to any other partner RP sites in order to avoid needing to re-authenticate.

Users, however, tend to navigate between sites using bookmarks, direct URL navigation, shared links, or search results. If they continue to behave this way, the current ID Bridge method will not change their traversal experience—they will continue to need to authenticate with each traversal. The only way that the current 'active' link method can effectively achieve the goal of smooth traversal is if users change their behavior. This is disadvantageous not only because of the difficulty of changing user behavior, but also because it stands in contrast to other prevalent Federated SSO systems that provide smoother traversal experiences, such as Facebook. In addition to reflecting poorly on the ID Bridge IdM system, these other Federated SSO systems make it even more unlikely that users will modify their behavior, as their current behavior is constantly reinforced by these other systems.

> *"SSO is an all-time favorite for end users. Using a single set of credentials for different Web sites without being reproached for it? Typing stuff only once? Count me in! ... You'll find that ... everybody will have a clear, intuitive understanding and appreciation of SSO. Perhaps not surprisingly, SSO became the Holy Grail of the industry long before the emergence of claims-based identity, and as of today a lot of people think that the ultimate goal of identity management should be universal SSO."*

—Vittorio Bertocci, Microsoft WIF Engineer & Evangelist[9]

Implementation

In addition to the difficulties experienced from the end-user's perspective, the current 'active' link method places additional burdens on partners, including:

- securing the pathways between all RPs and applications (e.g.: through firewall rules);
- modifying their systems to retain and track STS tokens in order to construct links to partner applications; and
- incurring the overhead of implementing the SOAP framework to be able to call the Bridge's validateToken() web service method.

The proposed use of the Federated SSO features already built into the ID Bridge's underlying WIF framework vastly simplifies the implementation work for partners by utilizing much of the same code that is already required for the basic 'primary' RP interaction with the ID Bridge. The following table compares the steps of the 'primary' authentication use case (in which a user travels directly from an RP to the bridge to authenticate and access that RP) to the steps of the 'secondary' authentication use case (in which a user who has already completed the 'primary' authentication use case traverses to a secondary RP):

RP – Originator / 'Primary' Authentication Use Case *(Current Functionality)*	**RP – Traversal / 'Secondary' Authentication Use Case *(Proposed Functionality)***
1a. . . . *User authenticates to **RP** via Bridge via selected IdP*	**1b.** . . . *User completes 'primary' authentication use case for **RP1** via Bridge via selected IdP*
	2b. User utilizes ***Passive Link*** *("plain-old" HTML link, bookmarked link, or types a URL)* to access a second **RP2** application.
	3b. *<background>* **RP2** application redirects to new validateViaCookie() endpoint on the **Bridge** – with return URL parameter – for validation.

[9] Vittorio Bertocci, "Advanced ASP.NET Programming: Single Sign-on, Single Sign-out, and Sessions," in *Programming Windows Identity Foundation* (Redmond, WA: Microsoft Press, 2011), https://ptgmedia.pearsoncmg.com/images/9780735627185/samplepages/9780735627185.pdf, 114-115.

	4b. <*background*> **Bridge's** validateViaCookie() endpoint executes nearly the same code as the existing validateToken() web service, except that the new code will first call WIF method TryReadSessionTokenFromCookie()
RP – Originator / 'Primary' Authentication Use Case *(Current Functionality)*	**RP – Traversal / 'Secondary' Authentication Use Case *(Proposed Functionality)***
2a. <*background*> **Bridge** posts the **User's** Identity Claims and STS Token in SAML assertion format to **RP** at the return endpoint URL.	**5b.** <*background*> **Bridge** returns **User's** Identity Claims and STS Token in SAML assertion format to **RP2** at the return endpoint URL.
3a. <*background*> **RP** web app unpacks SAML assertion to access Identity Claims.	**6b.** <*background*> **RP2** web app unpacks SAML assertion to access Identity Claims.
4a. <*background*> **RP** web app – in the simplest (happy path) case – checks if userID in the Claims is linked with existing **RP** account and allows **User** into **RP** application.	**7b.** <*background*> **RP2** web app – in the simplest (happy path) case – checks if userID in the Claims is linked with existing **RP2** account and allows **User** into **RP2** application.
5a. <*background*> **RP** should generate a "local" login with a "local" sessionID – i.e. a cached credential, in order to prevent having to redirect to the **Bridge** over and over again for validation.	**8b.** <*background*> **RP2** should generate a "local" login with a "local" sessionID – i.e. a cached credential, in order to prevent having to redirect to the **Bridge** over and over again for validation.

Implementing the use of session cookies for Federated SSO in the ID Bridge system requires partners to complete little work in addition to that already required for basic integration (the integration required to complete the 'primary' authentication use case). In the above table, the steps highlighted in green rely on the same code. Steps 5b and 2a both result in a SAML assertion being returned to the RP, and steps 6b, 7b, and 8b utilize the exact same code as steps 3a, 4a, and 5a (respectively) to read and process that assertion.

Steps 2b, 3b, and 4b are the only new steps needed for partners to take advantage of the proposed Federated SSO. Step 2b does not require additional work by partners (users may use their own links or bookmarks), but if some partners wish to include links to other partner RPs, embedding standard 'passive' HTML links is far simpler than creating the 'active' links required by the

current traversal method. Step 3b only requires writing code for a simple redirect to the ID Bridge. Step 4b is executed by the ID Bridge, and does not require additional work by partners.

The only real work that is required of partner RPs under the proposed Federated SSO is writing a few lines of code for a redirect to the ID Bridge. Compared to the current traversal method, this method greatly reduces the burden of implementation for partner. Not only does it eliminate the need to program complex 'active' links, but partners are also no longer required to track STS tokens or to implement SOAP or WS-Federation, removing the burden of implementing those service libraries and protocols.

> *"The good news? As long as the STS creates a session in its authentication method, having SSO across Web site RPs protected via WIF is something that works right out of the box. There's no arcane WS-Federation trick here, just good old cookies and a bit of trust management."*
>
> — Vittorio Bertocci, Microsoft WIF Engineer & Evangelist[10]

Adoption

A Federated IdM system for the environmental community works best with participation from a large number of states, tribes, and localities.[11] Without large-scale adoption, the benefits of this system to both partners and end-users are limited. Both the usability of the system and the ease of implementation have a strong impact on whether an environmental agency will choose to participate. A good end-user experience motivates potential partners to provide that experience to their user base, and an easy implementation is more likely to be quickly adopted. As more partners join, the benefits of participation increase for all.

But the current 'active' link system of traversal provides a corresponding disadvantage to large-scale adoption, as it does not scale well. If using this method, each change within the IdM system creates additional work for all partners (the 'n^2 problem'). For example:

- Each time a new partner joins, all partners must add it to 'whitelist' firewall rules.
- Each time a partner leaves, all partners must remove it from 'whitelist' firewall rules.
- Each time a domain changes, all partners must update their 'whitelist' firewall rules.
- All partners must maintain the 'active' link coding.

As more partners join the system, more work is required of both them and all the existing partners—the burden on partners (both in terms of effort and costs to hire contractors if necessary)[12] increases with the number of partners. This burden also increases the chance of

[10] Ibid., 115.
[11] "E-Enterprise Shared Identity Concept of Operations," 35.
[12] NMED's experience with the ISOL project has shown that some states do not have the necessary staff expertise to complete the technical work required to integrate with the ID Bridge, and thus will need to hire outside contractors.

mistakes: changes are more likely to be missed, resulting in security risks and/or broken links. This is a change management and governance challenge that only increases as participation increases. At some point (a 'point of diminishing returns'), the likelihood of potential partners joining (as well as existing partners continuing to participate) decreases due to the difficulty of implementation and maintenance. The benefits of large-scale adoption will be much harder to achieve with this barrier in place.

The proposed use of the 'passive' link method, however, eliminates this impediment to adoption. A Federated SSO based on the ID Bridge's existing WIF framework scales linearly, as RPs communicate solely with the ID Bridge, and not each other. Each partner RP that joins the trust framework requires only a single firewall rule for communication with the ID Bridge, which is already required to allow the basic ID Bridge functionality of authentication.

The proposed use of WIF Federated SSO via session cookies also aligns with existing Microsoft standards for Federated SSO as implemented by WIF.

Security

The proposed method of implementing Federated SSO is widely regarded as secure. The proposed usage of WIF Federated SSO via session cookies is in line with its standard usage. Microsoft O365 and Sharepoint both employ WIF for this exact purpose.

In addition, a 'passive' link method that utilizes cookies to support a Federated SSO system is not unique to WIF. It is also the methodology employed by other Federated SSO industry-standard frameworks, such as:

- OpenID Connect (used by Google)
- Facebook Federated SSO
- Java Spring Security
- Gluu
- Ping Identity
- Oracle IdM
- Okta

The current 'active' link method and the proposed use of 'passive' links with session cookies are both highly secure methodologies that share many similar security features. HTTPS is used to protect the entire process under both methodologies, and the STS token encryption, signature, and timeout are unchanged by the choice of methodology. While the 'active' link method uses secure SOAP protocol to return claims to the secondary RP from the validateToken() web

service, the proposed new method (in which the claims are posted to the secondary RP from the ID Bridge) is made equivalently secure through the use of encrypted, signed SAML assertions.

However, there are three small but notable differences in security between the two methodologies: the firewall rules ('whitelist') that must be created and maintained by all partner RPs, the mechanism of token transport, and the location of token storage.

Firewall Rules

The most significant of these differences is found in the requirements for RPs' firewall rules. As discussed in the Adoption section (above), the burden on an RP of maintaining firewall rules for all other RP applications in a large-scale trust framework increases the probability that vulnerabilities will be created through mistakes, oversights, or shortcuts taken to try to decrease this burden. For example, if an RP leaves the trust framework and another RP neglects to remove it from its 'whitelist,' the system is left open to an insider attack from the RP that left the framework. The proposed usage of WIF Federated SSO, however, only requires that an RP maintain a single firewall rule to the ID Bridge. In this system, only the ID Bridge would be responsible for revoking access by an RP that leaves the trust framework.

Token Transport

The proposed 'passive' link via session cookies methodology also uses a slightly more secure mechanism to transport the STS token than the current 'active' link method employs. The current system routes the token from the first RP to the second before sending it to the ID Bridge to be validated. While the second RP uses the highly secure validateToken() SOAP web service method to transport the token to the ID Bridge, the path between the two RPs is less secure because it is a simple post. On the other hand, the proposed usage of session cookies only requires the token (inside the cookie) be routed from the browser to the ID Bridge for validation. This method of transport is inherently secure because fundamental web and browser architecture only allows the cookie to be read by the domain that created it—in this case, the ID Bridge.[13]

Taken on its own, the current method of token transport has comparable security with the proposed method, as they are equivalently susceptible to man-in-the-middle (mitm) attacks at the https/ssl layer; however, the potential vulnerabilities created by inadequate maintenance of firewall rules compounds the risk of an mitm attack. The additional vulnerability created by the

[13] A. Barth, "HTTP State Management Mechanism," *Internet Engineering Task Force (IETF)*, April 2011, https://tools.ietf.org/html/rfc6265#, 11-12. During testing, NMED was able to verify the existence of session cookies created by the ID Bridge, but our RP was unable to read them, validating that partners cannot access these cookies.

need to maintain burdensome firewall rules does not exist in the proposed usage of the WIF Federated SSO via session tokens.

Token Storage

The final distinction between the two methodologies lies in the mechanism of token storage. In the current method, the token is stored in RP servers, while in the proposed new method, it is stored within a session cookie on the user's machine. This is marginally less secure, as someone who accessed the user's computer could potentially steal the cookie; however, the time-outs for both the session cookie and the token make this risk minimal. In addition, WIF offers the option to store session cookies on the ID Bridge and have the session cookie stored in the browser merely be a pointer, almost entirely eliminating that risk.[14]

Conclusion

The current method of RP traversal in the ID Bridge system has some significant disadvantages. Most significantly, the use case of truly seamless traversal between RPs can only be achieved if users modify their normal online behavior—something that is unlikely to occur. In addition, the burden on partner RPs is higher than it needs to be. These issues alone could impede large-scale adoption, but the fact that such adoption also both increases the burden on RPs and exacerbates security flaws creates an even more significant barrier to adoption.

The proposed use of WIF Federated SSO via session cookies utilizes pre-existing, standard features to help resolve these issues. This method allows users to maintain their normal online habits, decreases the work required of partner RPs, scales in a method that encourages and promotes large-scale adoption, and improves the Federated IdM system's overall security. Because these features are already included in the WIF framework, enabling their use in the ID Bridge should be straightforward. This small change to the ID Bridge will have significant benefits to its overall identity ecosystem.

[14] Vittorio Bertocci, "Your FedAuth Cookies on a Diet: IsSessionMode=true," *Cloud Identity*, May 26, 2010, http://www.cloudidentity.com/blog/2010/05/26/your-fedauth-cookies-on-a-diet-issessionmode-true/.

Additional Resources

The following resources provide additional information and detail on the topics discussed here:

- **Programming Windows Identity Foundation** – *Microsoft Press*
  - https://ptgmedia.pearsoncmg.com/images/9780735627185/samplepages/9780735627185.pdf (free download)
  - *See especially Chapter 4, pages 112-125: "Single Sign-on, Single Sign-out, and Sessions"*
- **A Guide to Claims-Based Identity and Access Control: Authentication and Authorization for Services and the Web (Microsoft patterns & practices)** – *Microsoft Press*
  - https://www.microsoft.com/en-us/download/details.aspx?id=28362 (free download)
  - *See especially:*
    - *Chapter 2, pages 20-22: "Browser-Based Applications"*
    - *Appendix B "Message Sequences", pages 239-251*
      - Provides particularly outstanding detail with diagrams and step-by-step analysis of the HTTPS traffic and how the WIF FedAuth session cookies are securely routed and validated.
    - *Chapter 11, "Claims-Based Single Sign-On for Microsoft SharePoint 2010"*
    - *Chapter 12, "Federated Identity for SharePoint Applications"*

Appendix E - Recommendations Document sent to E-Enterprise Management Board on July 14, 2017

The E-Enterprise Identity Solution (ISOL) Project Recommendations

Background

The mission of the Exchange Network grant-funded E-Enterprise Identity Solution (ISOL) Project for Phase I is to test out the process of integrating three very different State Partners – comprising a variety of Identity Management (IdM) systems and web applications – with the EPA developed Identity Bridge. The Identity Bridge was developed to provide the centralized component for a Federated Identity Management (FIdM) system for the E-Enterprise for the Environment ecosystem. This FIdM system establishes a trust framework among co-regulator Partners comprised of EPA, state, local and tribes and will be referred to in this document as the E-Enterprise Identity Management system (EEIdM) as described in the E-Enterprise Shared Identity Management Concept of Operations document. This document has been attached for reference.

Through the experience of this EEIdM integration work, the team identified opportunities for improvement of the current systems, trust framework, and architecture. In determining recommended improvements resulting from this project work the following criteria were used:

- Reduce burden of EEIdM integration for the Partners
- Enhance the user experience
- Increase adoption among Partners
- Ensure safe and secure interactions within the federated ecosystem.

The Identity Bridge has a very flexible and capable architecture and it is based on mature and proven standards and technologies. These include WS-Trust, WS-Federation, SAML 2, and Windows Identity Foundation (WIF), which is now part of the Microsoft .NET Framework. The Identity Bridge provides these broad capabilities:

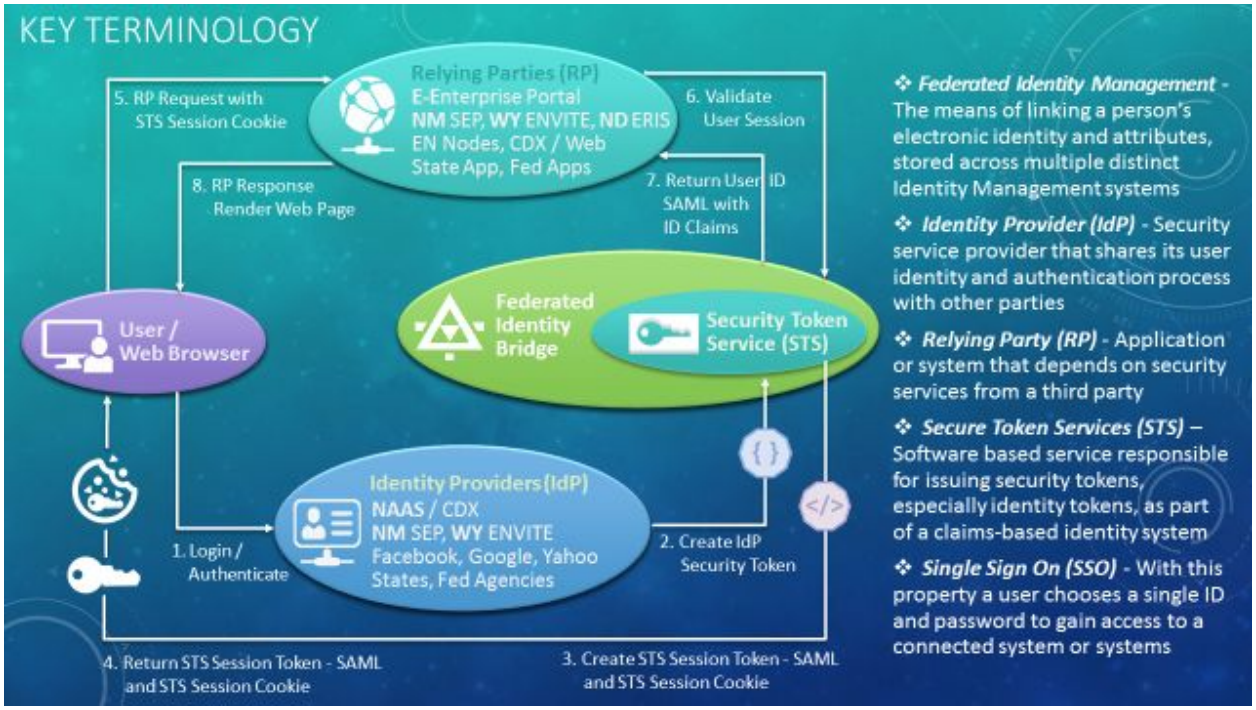
- Creates a Trust Framework between (potentially many) partner Identity Management (IdM) systems for authentication
- Supports services for Single Sign-On across E-Enterprise for the Environment
- Provides shared services for Authentication and context setting
- Supports seamless navigation across applications/domains

- Applications continue to Authorize users, but they should not need to Authenticate them or create new identity stores

The Identity Bridge architecture is comprised of several major components:

- *Identity Federation Multi-Protocol Processor:* Supports various security protocols such as OpenID Connect (OIDC), OpenID, OAuth, Attribute Exchange (AX), Live ID, etc.
- *OpenID Bridge:* Consists of an OpenID provider interface, an OpenID relying party interface and a user authentication interface
- *Security Token Services (STS):* Issues and validates Exchange Network tokens, SAML tokens and OpenID tickets – and provides access via Web Services APIs
- *Token Life-cycle Management Services:* Manages security tokens (reissuing, renewing, rebinding and revoking)
- *Attribute Mapping Services:* Translates, maps and converts user attributes between provider and relying parties NOTE: This functionality was not tested during this project.
- *EN OpenID Identity Provider (IdP):* Converts all Exchange Network user accounts into OpenID accounts; leverages Exchange Network identity management system
- *Role-based Security Policy Services:* Manages role-based authorization policies using web services which are enforced during token validation. NOTE: This functionality was not tested during this project since none of the participating partners required this capability.

The other two high-level components of the overall E-Enterprise Identity Management (EEIdM) architecture are the Identity Providers (IdP) and the Relying Parties (RP) as shown in the following Key Terminology diagram. Each of the EEIdM Partners (states, tribes, municipalities, federal agencies, web applications, etc.) may participate in the Federated Identity Management Trust Framework as an IdP, an RP, or both. Additionally, social media IdPs (e.g. Login with Facebook) may participate at a low-trust Level of Assurance (LOA).



We evaluated the experience of four Partners: E-Enterprise Portal (RP), NMED SEP (IdP & RP), WY DEQ ENVITE (IdP & RP), and ND DoH ERIS (RP). Note that the E-E Portal and ERIS are individual web applications, while SEP and ENVITE are Single Sign-On (SSO) gateways for multiple web applications. Based on these experiences we have developed the following recommendations for best practices and suggested improvements.

Identity Provider (IdP) Recommendations

All Partners in the federated trust framework should standardize the set of Identity Claims through mutual agreement. This would then apply to all Partners providing IdP services. The set of standardized claims should be as small as possible, consisting of the minimum claims needed both technically and for efficient governance. Technically required claims include only:

- Email Address (which serves as the federated ID)
- Given Name (commonly the person's first name)
- Family name (commonly the person's last name)
- Username

Claims helpful for governance purposes include:

- Organization
- Title
- Phone
- Address
- Level of Assurance (LOA)

- CROMERR-compliance flag
- IdP used

External IdPs within the EEIdM framework, such as Facebook, Google, Twitter, etc. should have their identity claims "mapped" to the agreed standard claims within EEIdM. The Identity Bridge already provides such an Attribute-Mapping (claim-mapping) feature that can be leveraged for this purpose.

We recommend the Bridge's claim-mapping feature be used – and if need be – technically extended, to enforce the standardization of identity claims across all the IdPs in the EEIdM system. Additional IdP-specific claims can still be allowed, such as Facebook profile information. However, the core claims should be standardized to reduce the burden on Relying Parties (RPs) as much as possible. In the big-picture sense, this will ensure that the EEIdM system remains scalable.

During the integration efforts of the ISOL proof-of-concept project each RP had to write additional code to handle the differing identity claims from different IdPs. This burden will only increase as new IdPs are added to the EEIdM framework unless standardized claims are mandated.

It may become necessary or desirable to add additional identity claims in the future, or to modify or add Identity Provider protocols. Because of the significant impact of such changes to the Partners in the EEIdM system, governance policy and governance structures (e.g. a management board) need to be put in place to ensure smooth transitions and minimal disruptions as these modifications to the overall system are deployed.

Relying Party (RP) Recommendations

The flip-side of requiring each IdP in the EEIdM framework to use a standardized set of identity claims is for the Relying Party (RP) web applications to utilize these standard claims in a consistent manner. For example, each RP must utilize the email claim as the federated ID. And conversely, they must ***not*** use some other claim (or combination of claims) as a federated ID.

EEIdM governance should develop Partner agreements to handle some aspects of authorization in an appropriate standardized manner. Claims such as level of assurance (LOA) and CROMERR-compliance flag (a yes/no value) need to be defined and documented through Partner agreements as part of this governance. Guidance as to what aspects of the claims such as LOA and IdP CROMERR flag can be used by the RP as supporting information to make decisions for authorized access to systems and resources. For example, if the user was authenticated by an IdP that is CROMERR certified, could the RP verify that a physical signature for that user is on file by contacting the IdP or would another physical signature be required?

Identity Bridge Recommendations

The Bridge set of supported claims should be extended to those claims agreed on by the ISOL governance entity, which might include the following claims:

- Organization
- Title
- Phone
- Address
- Level of Assurance (LOA)
- CROMERR-compliance flag
- IdP used

As mentioned previously, we recommend the Bridge's claim-mapping feature be used – and if need be – technically extended to enforce the standardization of all EEIdM core identity claims across all the IdPs in the EEIdM framework. This will have the greatest effect toward reducing the burden on RPs to allow seamless traversal from any other RP in the EEIdM trust framework.

For external IdPs, such as Facebook, Google, Yahoo, etc., the Bridge should always set an appropriately low Level of Assurance (LOA) claim (i.e. a LOA of 1 on a scale of 1-4). An LOA value of 1 is appropriate for access by the general public on the open internet. Also as mentioned previously in the Identity Provider section, external IdPs within the EEIdM framework, such as Facebook, Google, Twitter, etc. should have their identity claims "mapped" to the agreed-upon standard claims within the EEIdM.

Such general users should only be allowed access to public facing web pages by any RP in the EEIdM framework. Public access users might be allowed a limited feature set such as the ability to open record requests, customize their user profile, or create public comments.

In a similar manner for users logging in with an external IdP, the Bridge should always ensure that the CROMERR-Compliance flag claim be set with a value of "No". Any future additions to the common set of claims relating to authorization would likewise default to the most limited access for any public user who logged in via an external IdP.

The Identity Bridge should be modified to include additional URL endpoints in support of passive traversal within EEIdM. Discussions around providing this functionality have taken place with OEI and research is underway to determine the amount of effort that would be required to implement this capability. Below is a summary of the topic and recommendation. The NM project team produced a white paper titled, "EPA Identity Bridge – Proposal for Federated Single Sign On", that was presented to OEI. It is provided for reference.

EPA Identity Bridge – Proposal for Federated Single Sign On

The ability for users to traverse smoothly from one Relying Party (RP) to another without needing to re-authenticate is an expected and desirable function of a Federated Identity Management (IdM) system. The E-Enterprise Shared Identity Management Concept of Operations (ConOps) identifies a "seamless user experience between partner systems and

services" as one of the "primary benefits" of such a system. The EPA's Identity (ID) Bridge system was designed to meet the requirements laid out in the ConOps, and currently employs a method of RP traversal in which RPs create 'active' links that post Secure Token Services (STS) Tokens to other RPs. The RP that receives an STS Token then invokes the Bridge web service method validateToken(). Although this allows smooth traversal, it both requires significant work for partner RPs to implement and maintain these links and necessitates that users modify their online navigation habits to utilize them.

The team in its implementation of traversal became aware that the current implementation of the Identity Bridge implements passive links via session cookies placed within the user's browser. However, the Relying Party has no way of determining whether the user has a valid token or is visiting the site for the very first time since the Relying Party cannot interrogate the session cookie since it belongs to the Bridge. This is a reasonable and important security feature. One way to take advantage of the session cookie and enable smooth traversal without users having to click through to their desired application is for the ID Bridge to implement URL endpoints that the Relying Party can redirect the user's browser to for validation by the session cookie owner, the Identity Bridge. The URL endpoints that are recommended for implementation by the Identity Bridge would be: one to validate the session cookie, one to renew the session cookie and one to remove the session cookie.

More information on this recommendation can be provided by the ISOL project team and by the Identity Bridge development team.

Governance Recommendations:

The recommended EEIdM governance requirements for moving to a production system are comprised of three broad categories: Operations & Support Procedures, Standards & Policies and Research & Development

- Operations & Support
    - EIdM Change Management Process (including the Identity Bridge)
        - Change management process to ensure communication and participation by all EEIdM partners in the modification and maintenance of the software components. Focus is on the system distributions that have an impact on delivery service to participants including and likely most importantly, the Identity Bridge.
    - Notification and communication mechanism when new IdPs and RPs are added or removed from the trust network
    - Tech support for the Identity Bridge and its components for setup, testing and troubleshooting issues
    - Partner communication forum to discuss integration issues, policy issues, connectivity issues, new design approaches, etc.
    - Provide new partner training and integration assistance
    - Provide test processes to ensure proper connectivity to the system
    - Create and/or maintain technical documentation such as developer guides for IdP and RP roles for a variety of technical platforms

    - Collect metrics on usage to support decision making and priority setting
    - Perform active outreach to engage more partner interaction with the system
- Governance & Policies
    - IdP Standards
        - All Partners in the federated trust framework should standardize the set of Identity Claims per mutual agreement. See additional detail on this in the above section for Identity Providers.
    - RP Standards
        - Develop Partner policies/agreements to handle some aspects of authorization in an appropriate standardized manner. Relying Party (RP) web applications need to utilize IdP standard claims in a consistent manner. See additional detail on this in the above section for Relying Parties. Specific claims to be addressed include using email addresses as the federated ID, LOA claims and use of a CROMERR-compliance flag.
        - Policies should be established for Relying Parties to limit access for users authenticated using external External IdPs within the EEIdM framework, such as Facebook, Google, Twitter. This will support the concept of a trust framework among co-regulator partners.
    - Identity Bridge Improvements
        - Prioritization of Identity Bridge new feature development and management of the release cycle. See the *Identity Bridge Recommendations* section above.
    - Develop a new member Partner Agreement document that outlines terms of engagement within the systems and security requirements/verification for participation
    - Establish a Partner Adoption Strategy to include the collection of metrics of participation, sanctioned or EEIdM certified vendors for integration work, and goal setting for adoption
    - Develop a process and rules for terminating a participating partner
    - Develop an emergency process for removing potentially bad actor identities from the system
- Research & Development: Identify new features to improve the system overall
    - Research current industry trends and protocols to keep the system aligned with open standards and protocols
    - Investigate ways to leverage the Identity Bridge and Secure Token Services to secure APIs used between partner systems for programmatic data, document and map sharing
    - Investigate ways to leverage Shared CROMERR Services within the system to reduce the burden of implementing CROMERR requirements on partner systems
    - Investigate ways to integrate third party collaboration tools as Relying Parties into the system such as Google Docs and Sharepoint to promote increased secure collaborative work between co-regulators and the regulated community