Environmental Information exchange Network

EN2017

IDENTITY MANAGEMENT SOLUTIONS

AN EXCHANGE NETWORK PARTNERSHIP GRANT PROJECT

Mary Montoya, *New Mexico Environment Department*
Chris Clark, *U.S. EPA OEI*

2017 Exchange Network National Meeting

INNOVATION AND PARTNERSHIP

May 15-18, 2017
Sheraton Philadelphia Society Hill Hotel
Philadelphia, Pennsylvania

#EN2017
http://www.exchangenetwork.net/en2017

ABSTRACT

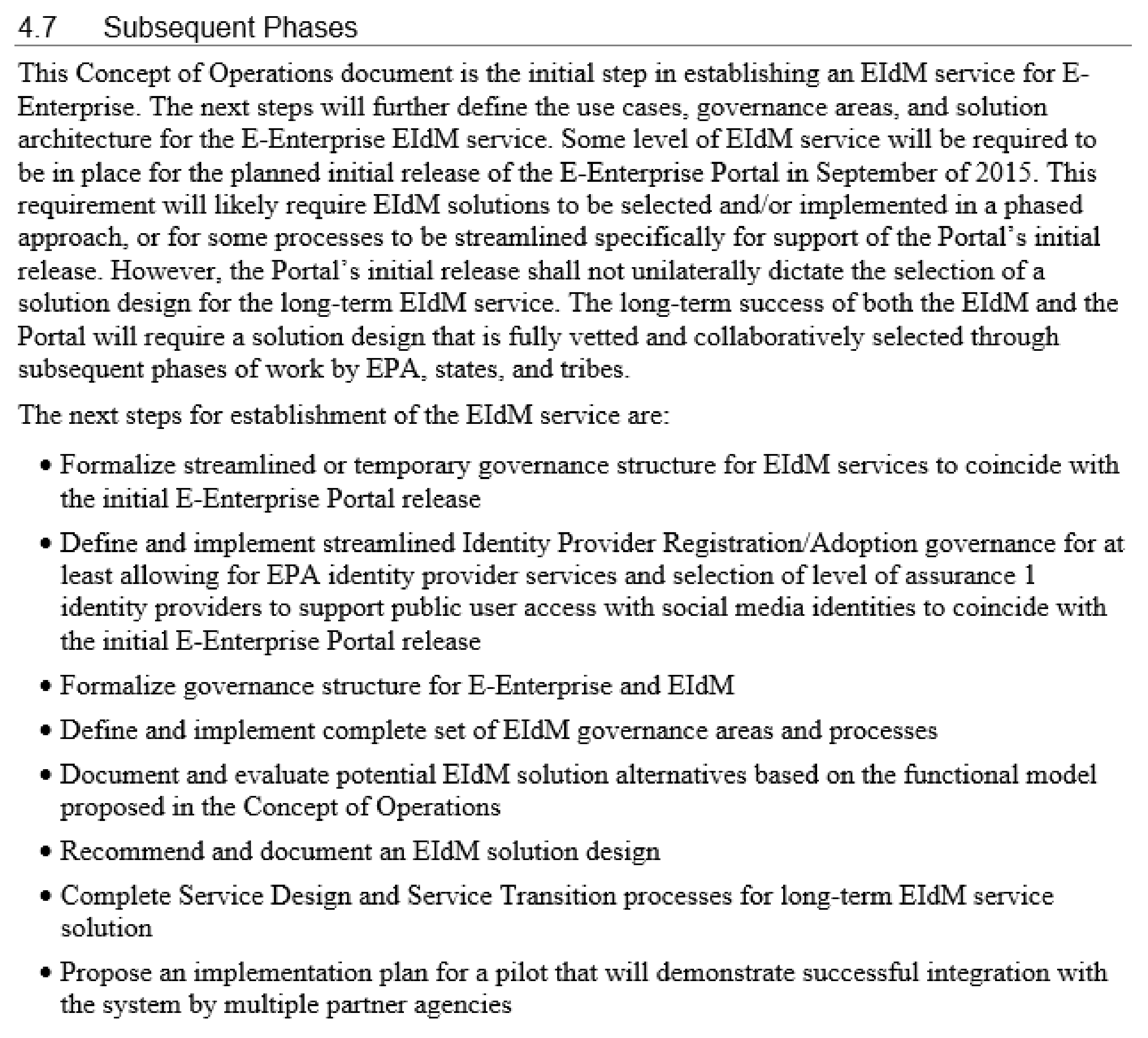
E-Enterprise partners are seeking new ways to offer more seamless and efficient user experiences to customers that do business with environmental agencies. This presentation will explore efforts by states and EPA to build a trusted framework that allows users to securely traverse between state systems and the E-Enterprise portal without the need to re-authenticate. The partners will describe their development experience, future plans, and benefits of participating in this trusted framework. The team will also describe proposed improvements to the system that would reduce the burden for participation, enhance the user experience, and ensure security.

AGENDA

- Project Background, Mission and Goals
- Our Partners
- Key Terminology
- Project Considerations / Partner Technology
- Demonstration
- Partner Experience / Future Plans
- Project Deliverables
- Project Recommendations
- Beyond Scope, Next Steps & Conclusion
- Q&A

PROJECT BACKGROUND

- E-Enterprise Shared Identity Management Concept of Operations document produced in June, 2015
  - Provided the blueprint for providing a seamless experience for users traversing between partner applications and the EE Portal
  - Section 4.7 (Subsequent Phases) identified the next steps for establishing an Enterprise Identity Management Service
- EPA developed the Identity Bridge to enable authentication options for users
- The Exchange Network Partnership Grant Project led by NMED started in October, 2015
  - Originally conducted Discovery Sessions with EPA and in New Mexico
  - Partnered with WY and ND for remainder of project
  - Planned, designed and implemented a proof of concept to verify a technical approach



4.7 Subsequent Phases

This Concept of Operations document is the initial step in establishing an EIdM service for E-Enterprise. The next steps will further define the use cases, governance areas, and solution architecture for the E-Enterprise EIdM service. Some level of EIdM service will be required to be in place for the planned initial release of the E-Enterprise Portal in September of 2015. This requirement will likely require EIdM solutions to be selected and/or implemented in a phased approach, or for some processes to be streamlined specifically for support of the Portal's initial release. However, the Portal's initial release shall not unilaterally dictate the selection of a solution design for the long-term EIdM service. The long-term success of both the EIdM and the Portal will require a solution design that is fully vetted and collaboratively selected through subsequent phases of work by EPA, states, and tribes.

The next steps for establishment of the EIdM service are:

- Formalize streamlined or temporary governance structure for EIdM services to coincide with the initial E-Enterprise Portal release
- Define and implement streamlined Identity Provider Registration/Adoption governance for at least allowing for EPA identity provider services and selection of level of assurance 1 identity providers to support public user access with social media identities to coincide with the initial E-Enterprise Portal release
- Formalize governance structure for E-Enterprise and EIdM
- Define and implement complete set of EIdM governance areas and processes
- Document and evaluate potential EIdM solution alternatives based on the functional model proposed in the Concept of Operations
- Recommend and document an EIdM solution design
- Complete Service Design and Service Transition processes for long-term EIdM service solution
- Propose an implementation plan for a pilot that will demonstrate successful integration with the system by multiple partner agencies

PROJECT MISSION STATEMENT

The mission of the E-Enterprise Identity Solution (ISOL) Project is to test out the process of integrating three very different State systems with the existing Identity Bridge which was developed to provide a federated identity 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

E-ENTERPRISE for the environment

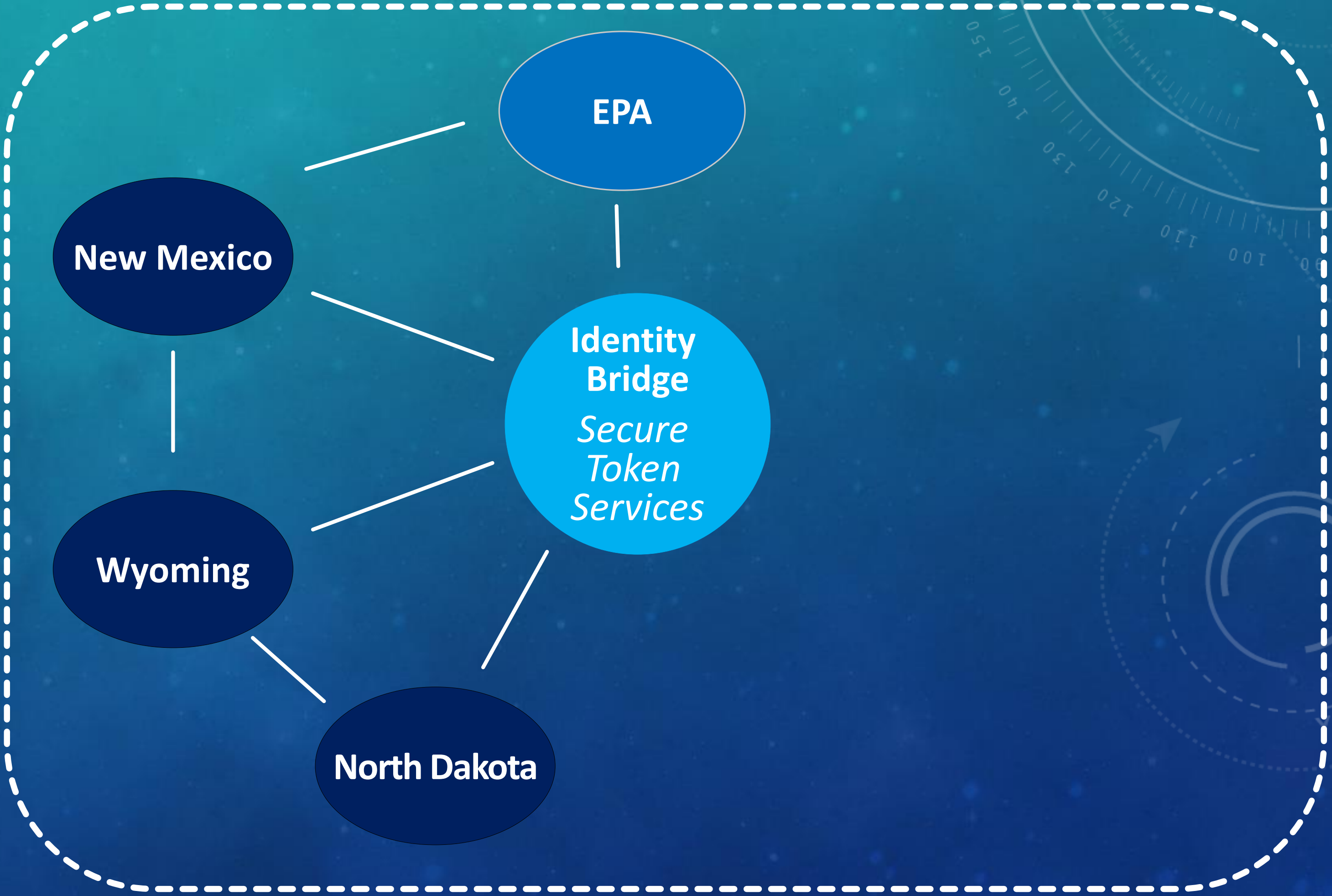
Federated Identity Management System

Main Goal:

Identify how best to authenticate users once and allow secure access to other related sites *without* reauthenticating

Future Aim:

Increase partner adoption which will facilitate transacting business among co-regulators and with the regulatory community



EPA

New Mexico

Identity Bridge

Secure Token Services

Wyoming

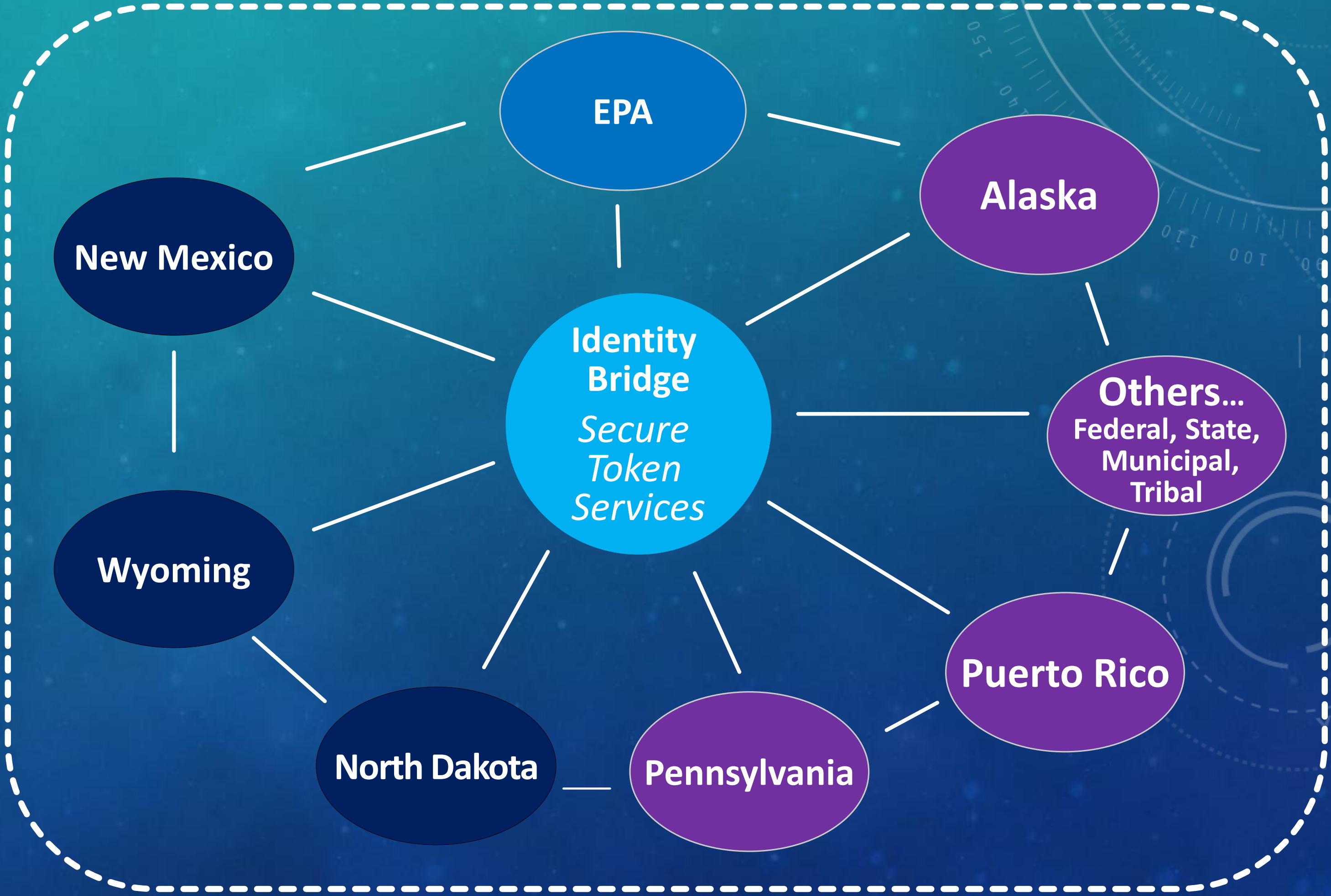
North Dakota

BENEFITS AND IMPACT

- Increased user privacy and security of user credentials
- Reduce cost and burden associated with maintaining multiple identities
- Increased accuracy and currency of user information (claims)
- Enhanced user experience (fewer passwords and seamless traversal)
- Promotes collaborative work between co-regulators, the regulated community and regional interests
- Broader and more secure access by co-regulators and the regulated community to more timely and accurate data across the Enterprise
- Potential impact to hundreds of co-regulators and tens of thousands of regulated entities

E-ENTERPRISE
for the environment

Federated Identity Management System



OUR PARTNERS

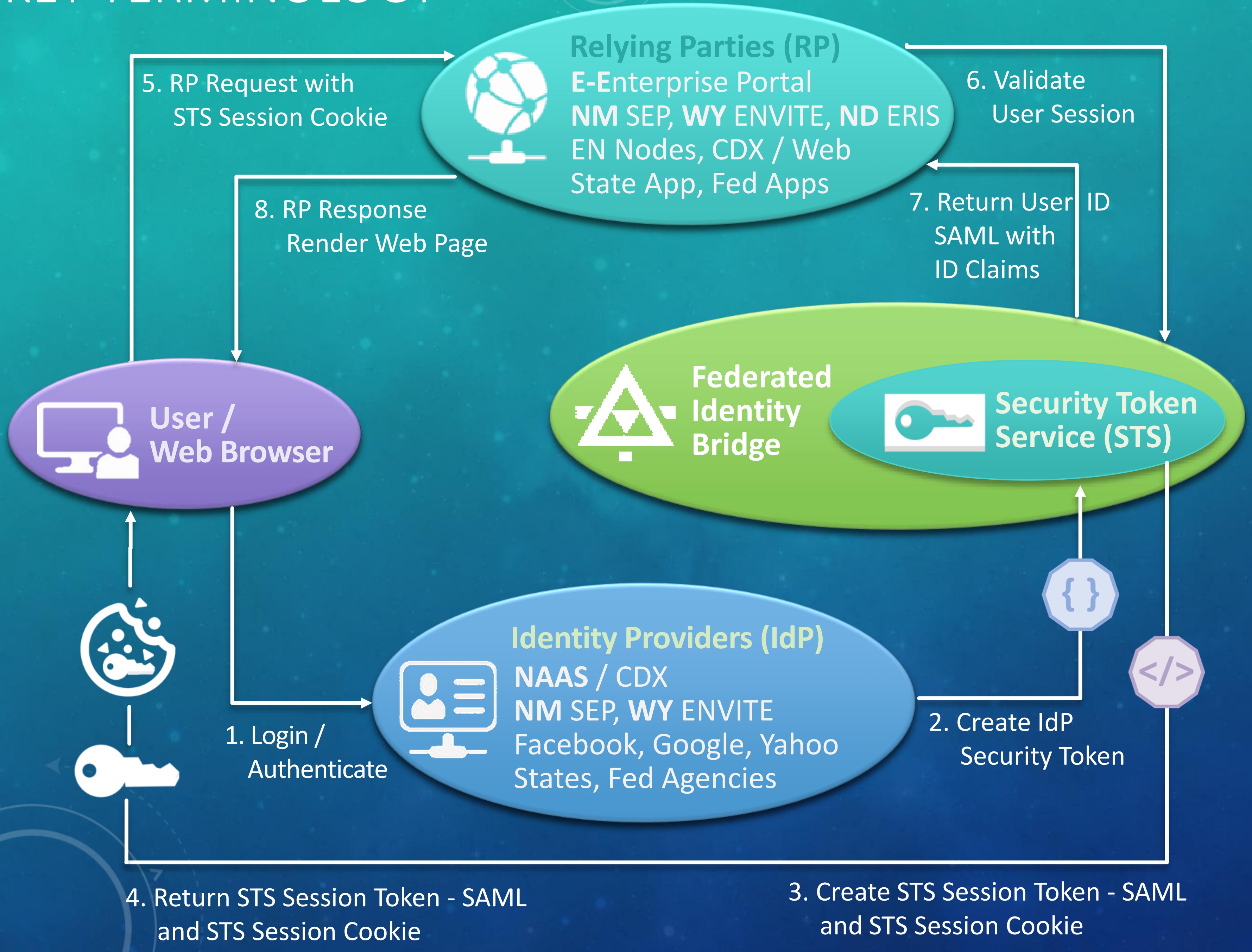
EPA

New Mexico

Wyoming

North Dakota

KEY TERMINOLOGY



Relying Parties (RP)

E-Enterprise Portal

NM SEP, **WY** ENVITE, **ND** ERIS

EN Nodes, CDX / Web

State App, Fed Apps

User / Web Browser

Federated Identity Bridge

Security Token Service (STS)

Identity Providers (IdP)

NAAS / CDX

NM SEP, **WY** ENVITE

Facebook, Google, Yahoo

States, Fed Agencies

1. Login / Authenticate

2. Create IdP Security Token

3. Create STS Session Token - SAML and STS Session Cookie

4. Return STS Session Token - SAML and STS Session Cookie

5. RP Request with STS Session Cookie

6. Validate User Session

7. Return User ID SAML with ID Claims

8. RP Response Render Web Page

❖ ***Federated Identity Management*** - The means of linking a person's electronic identity and attributes, stored across multiple distinct Identity Management systems

❖ ***Identity Provider (IdP)*** - Security service provider that shares its user identity and authentication process with other parties

❖ ***Relying Party (RP)*** - Application or system that depends on security services from a third party

❖ ***Secure Token Services (STS)*** – Software based service responsible for issuing security tokens, especially identity tokens, as part of a claims-based identity system

❖ ***Single Sign On (SSO)*** - With this property a user chooses a single ID and password to gain access to a connected system or systems

PROJECT CONSIDERATIONS

- Security-Related Concerns
  - Trust and Levels of Assurance from Identity Providers
- Openness, Flexibility and Standards
  - Modern and Widely-Adopted Standards
  - Decentralized Authentication Protocols
- Reduced Burden for Partners
  - Ease of Partner Integration, Implementation and Maintenance
  - Best End-User Experience
- Outreach
  - Documents and Tools For Successful Integration and Use
  - Technical vs. Non-Technical Hurdles

PARTNER TECHNOLOGY

Current Technology:

E-Enterprise Portal	**NM NMED** SEP	**WY WDEQ** ENVITE	**ND DoH** EHS ERIS
PHP	**Java EE**	**.NET** ***C#***	**.NET** *VB*
Apache	**Apache +** **Tomcat**	**MS IIS**	**MS IIS**
IdM ID Bridge, SimpleSAMLphp	**IdM** Oracle DB, Spring Security	**IdM** MS SQL DB, IdentityServer	**IdM** MS SQL DB, LDAP, Tivoli

Solution Required:

RP SOAP, SimpleSAMLphp	**RP** OpenSAML, Auth10, JAX-WS	**RP** .NET, WIF, SOAP, SAML	**RP** .NET, WIF, SOAP, SAML
IdP Exchange CDX *OpendID Token*	**IdP** phpOIDC OIDC *JWT Token*	**IdP** IdentyServer SAML2p *SAML Token*	T.B.D.

The ISOL Project is ***not*** a Replacement Solution

✓ Embraces the diversity of Partner's current web applications and identity management systems

✓ Leverages existing web technologies and identity systems as part of the solution

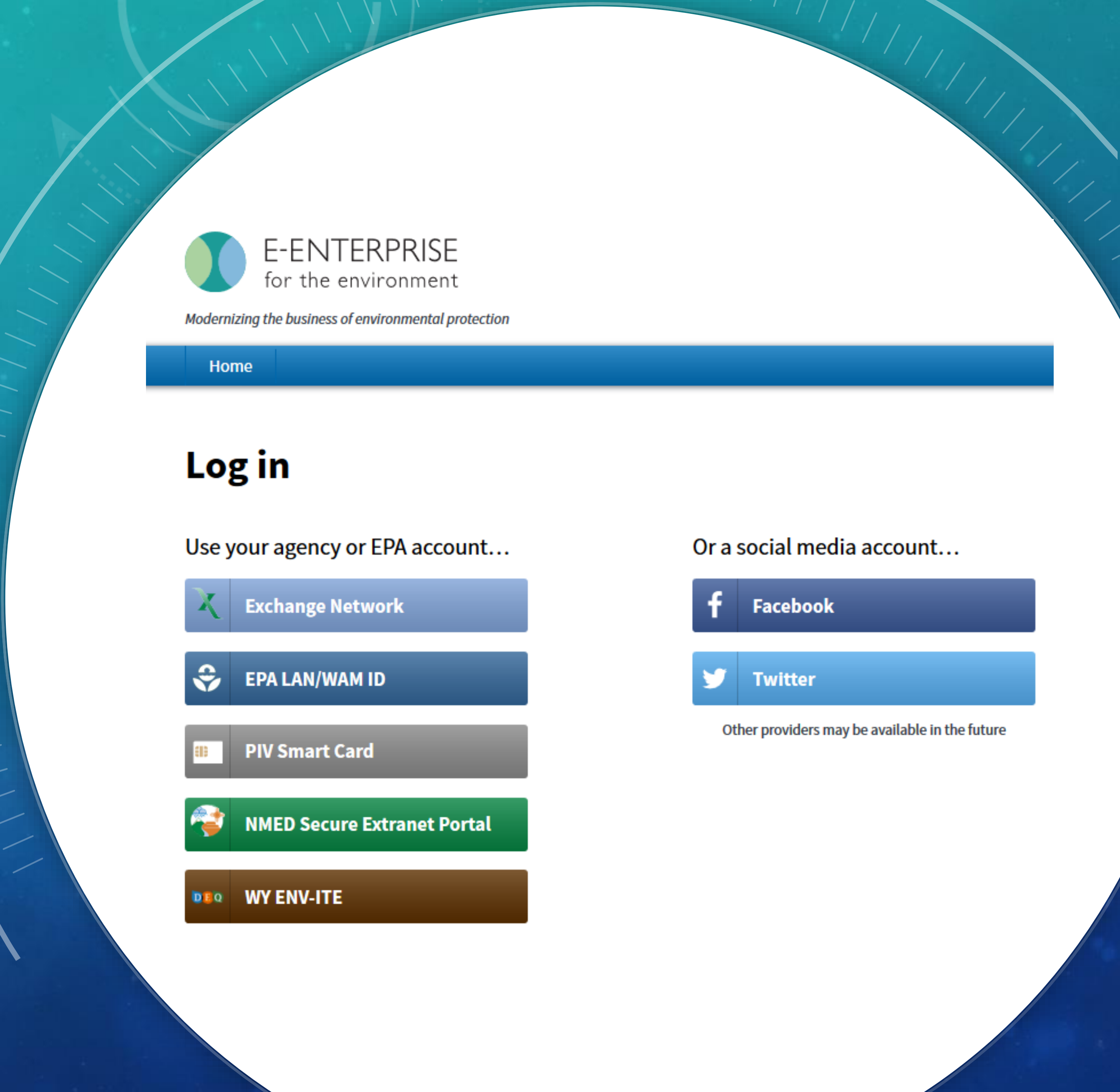
HYPOTHETICAL REAL LIFE STORIES

I. ACME Inc. has an Air Quality permit and a NPDES permit in a State where Air Quality is a delegated program to the State and Clean Water is not. ACME's staff logs into the State's application to report air emissions and then needs to traverse to the EPA Portal to obtain their NPDES permit information.

II. Utah is studying stream analytes for an Interstate Waterway that travels from New Mexico into the Navajo Nation and to Utah. An environmental scientist logs into Utah's water quality application for data, traverses to New Mexico for additional information and Navajo Nation's Tribal system for even more information. A more complete analysis can now be performed on the waterway.

III. EPA is working with Wyoming to reconcile air emissions submitted through the node. EPA staff log into CDX to access the reported data then traverse to the Wyoming's air emissions reporting application to compare data.

DEMONSTRATION



E-ENTERPRISE for the environment

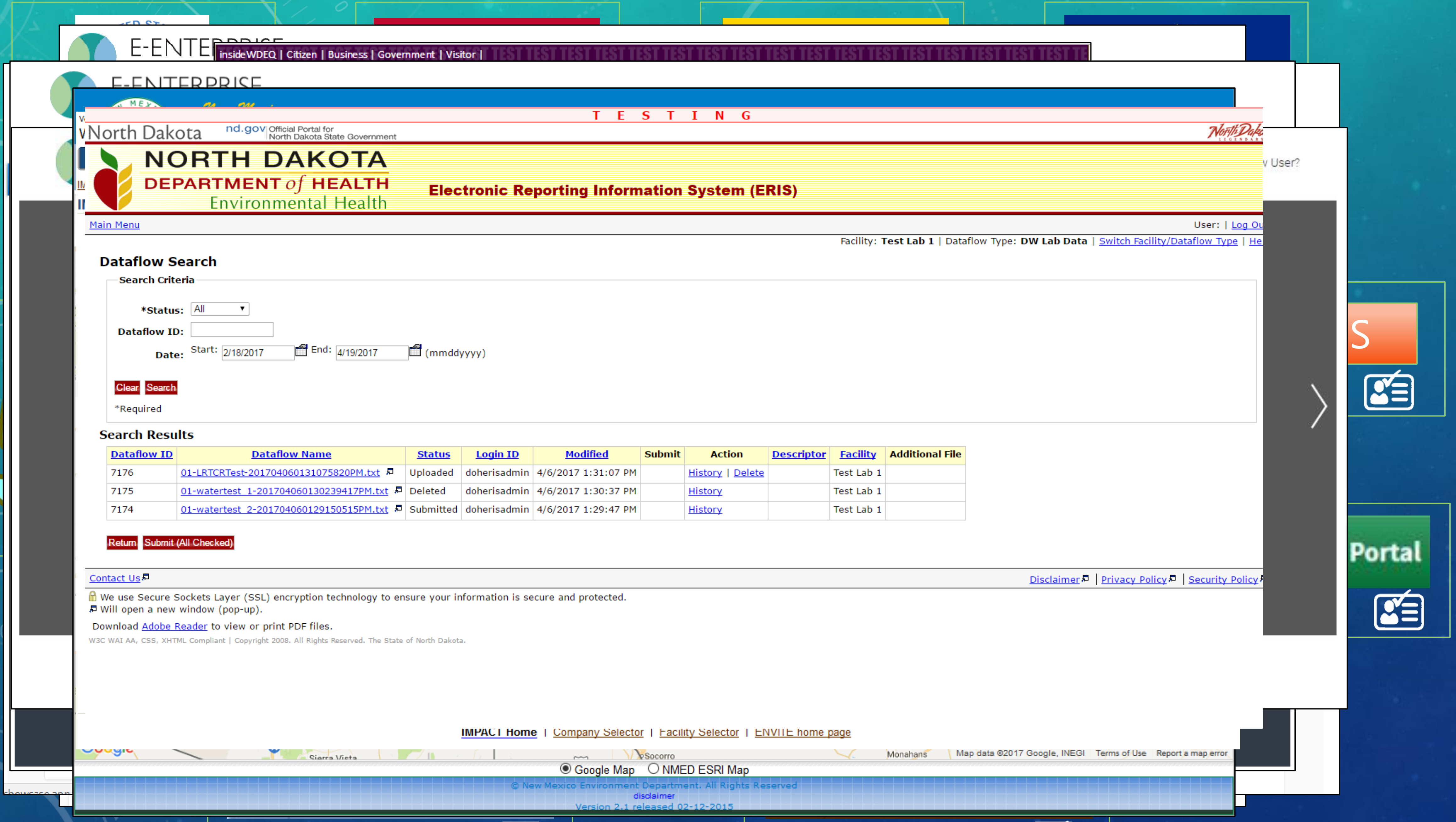
Modernizing the business of environmental protection

Log in

Use your agency or EPA account…

Or a social media account…

Other providers may be available in the future



TESTING

North Dakota nd.gov Official Portal for North Dakota State Government

NORTH DAKOTA DEPARTMENT of HEALTH Environmental Health

Electronic Reporting Information System (ERIS)

Main Menu | User: | Log Ou

Facility: **Test Lab 1** | Dataflow Type: **DW Lab Data** | Switch Facility/Dataflow Type | He

Dataflow Search

Search Criteria

***Status:** All

Dataflow ID:

Date: Start: 2/18/2017 End: 4/19/2017 (mmddyyyy)

Clear Search

*Required

Search Results

Dataflow ID	Dataflow Name	Status	Login ID	Modified	Submit	Action	Descriptor	Facility	Additional File
7176	01-LRTCRTest-201704060131075820PM.txt	Uploaded	doherisadmin	4/6/2017 1:31:07 PM		History | Delete		Test Lab 1	
7175	01-watertest_1-201704060130239417PM.txt	Deleted	doherisadmin	4/6/2017 1:30:37 PM		History		Test Lab 1	
7174	01-watertest_2-201704060129150515PM.txt	Submitted	doherisadmin	4/6/2017 1:29:47 PM		History		Test Lab 1	

Return Submit (All Checked)

Contact Us | Disclaimer | Privacy Policy | Security Policy

We use Secure Sockets Layer (SSL) encryption technology to ensure your information is secure and protected.
Will open a new window (pop-up).

Download Adobe Reader to view or print PDF files.

W3C WAI AA, CSS, XHTML Compliant | Copyright 2008. All Rights Reserved. The State of North Dakota.

IMPACT Home | Company Selector | Facility Selector | ENVITE home page

Map data ©2017 Google, INEGI Terms of Use Report a map error

● Google Map ○ NMED ESRI Map

© New Mexico Environment Department. All Rights Reserved
disclaimer
Version 2.1 released 02-12-2015

Identity Provider (IdP)

Identity Provider (IdP)
WY Validation

PARTNER STATUS – NEW MEXICO

- ✓ **Milestones:**
  - ✓ **Complete Discovery Sessions**
    - ✓ Analyze current technical platform including existing Identity Management framework
    - ✓ Determine the roles the partner would like to play in a Federated ID system

Complete

  - ✓ **Complete Gap Analysis**
    - ✓ Assess level-of-effort to integrate current system(s) with the EPA Identity Bridge

80% Complete

  - ✓ **Proof of Concept Feasibility**
    - ✓ Determine whether a prototype integration of the Identity Bridge is feasible

Complete

PARTNER STATUS – WYOMING

- ✓ **Milestones:**
  - ✓ **Complete Discovery Sessions**
    - ✓ Analyze current technical platform including existing Identity Management framework
    - ✓ Determine the roles the partner would like to play in a Federated ID system

    Complete
  - ✓ **Complete Gap Analysis**
    - ✓ Assess level-of-effort to integrate current system(s) with the EPA Identity Bridge

    75% Complete
  - ✓ **Proof of Concept Feasibility**
    - ✓ Determine whether a prototype integration of the Identity Bridge is feasible

    Complete

PARTNER STATUS – NORTH DAKOTA

- ✓ **Milestones:**
  - ✓ **Complete Discovery Sessions**
    - ✓ Analyze current technical platform including existing Identity Management framework
    - ✓ Determine the roles the partner would like to play in a Federated ID system

Complete

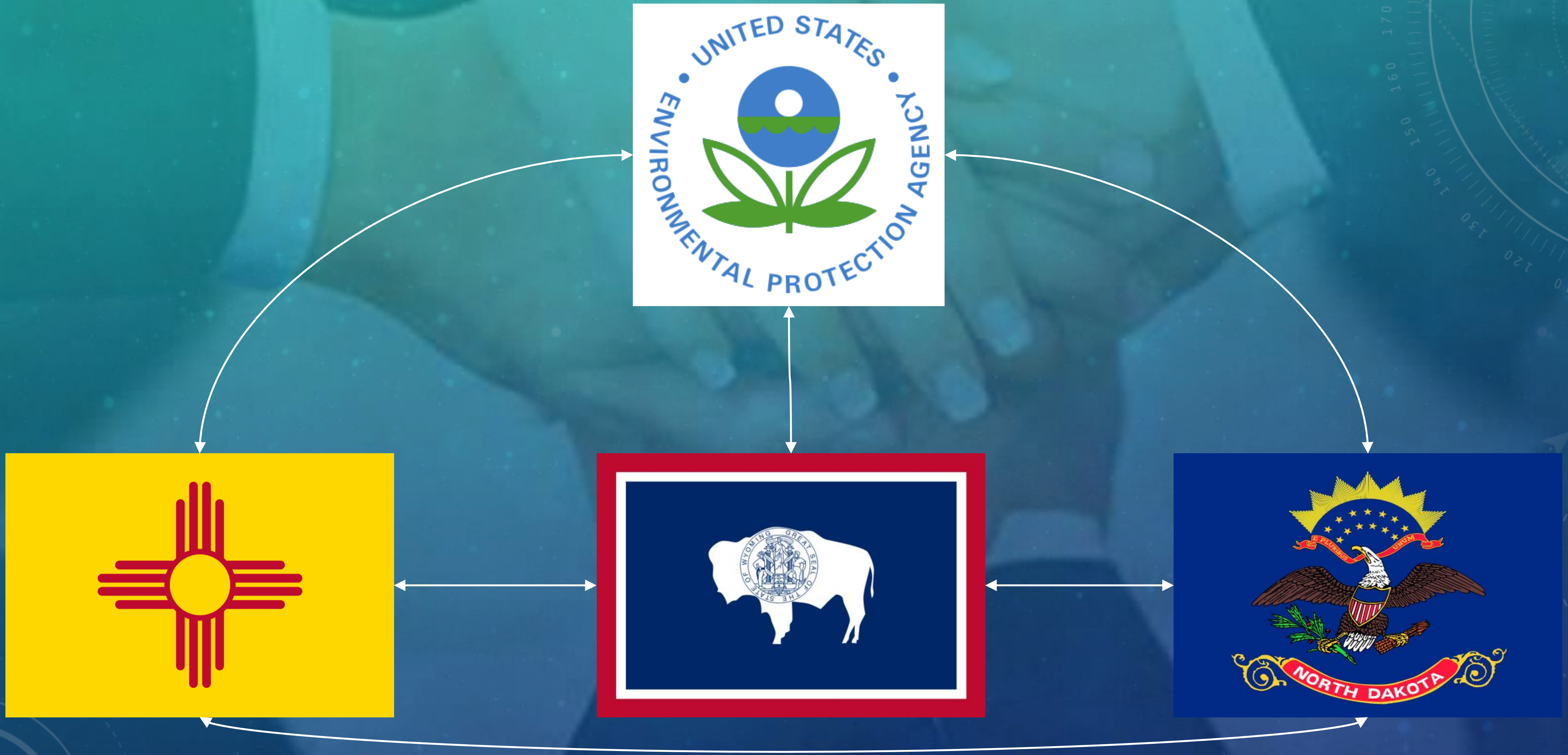
  - ✓ **Complete Gap Analysis**
    - ✓ Assess level-of-effort to integrate current system(s) with the EPA Identity Bridge

50% Complete

  - ✓ **Proof of Concept Feasibility**
    - ✓ Determine whether a prototype integration of the Identity Bridge is feasible

75% Complete

PARTNER EXPERIENCE


UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
GREAT SEAL OF THE STATE OF WYOMING
E PLURIBUS UNUM
NORTH DAKOTA

PARTNER EXPERIENCE

Steve Girt
WY Dept. of Environmental Quality

WYOMING OUTSIDE OF THE BOX

Wyoming’s ENVITE solution is a .Net CROMERR certified, single-sign on solution that serves the needs of Wyoming for its e-reporting and e-permitting needs.

With ENVITE, Wyoming’s user community have the ability to authenticate, e-sign and leverage tools from ENVITE for authorization into its applications as well as provide proof of signature of its documents and data that they have uploaded to SharePoint.

The New Mexico e-enterprise grant provided in cooperation with Wyoming, North Dakota and EPA has taken ENVITE from a stand alone Wyoming solution to proof of concept outside of the box!

WYOMING OUTSIDE OF THE BOX

From the proof-of-concept, Wyoming’s ENVITE solution now has the ability to provide industry users a seamless traversal between New Mexico, EPA and North Dakota.

In addition, industry users may authenticate to CDX, New Mexico, or North Dakota credentials and traverse to Wyoming applications through ENVITE to apply for a permit or e-sign data in Wyoming!

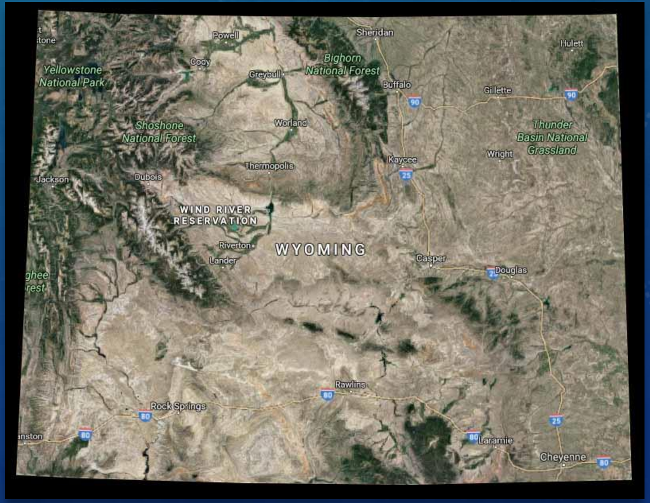
WYOMING OUTSIDE OF THE BOX

ENVITE was built on an open source identity platform called Identity Server. It supports a wide variety of standards and technologies.

Configuring ENVITE as a identity provider in the EPA's Identity Bridge was as simple as adding a line to a database table.

Configuring EPA's Identity Bridge as an identity provider in ENVITE required some minor development but was built in such a way that additional providers can be added through configuration.

Our contractor, Gannett Peak was able to accomplish the above within a month from the initiation of the contract.



WYOMING OUTSIDE OF THE BOX

The Future and Beyond!

From the proof-of-concept, Wyoming DEQ is interested in moving forward with the ability to leverage OpenID infrastructure such as Facebook, Google or Yahoo for tracking read-only authenticated users to our applications for records requests or public access.

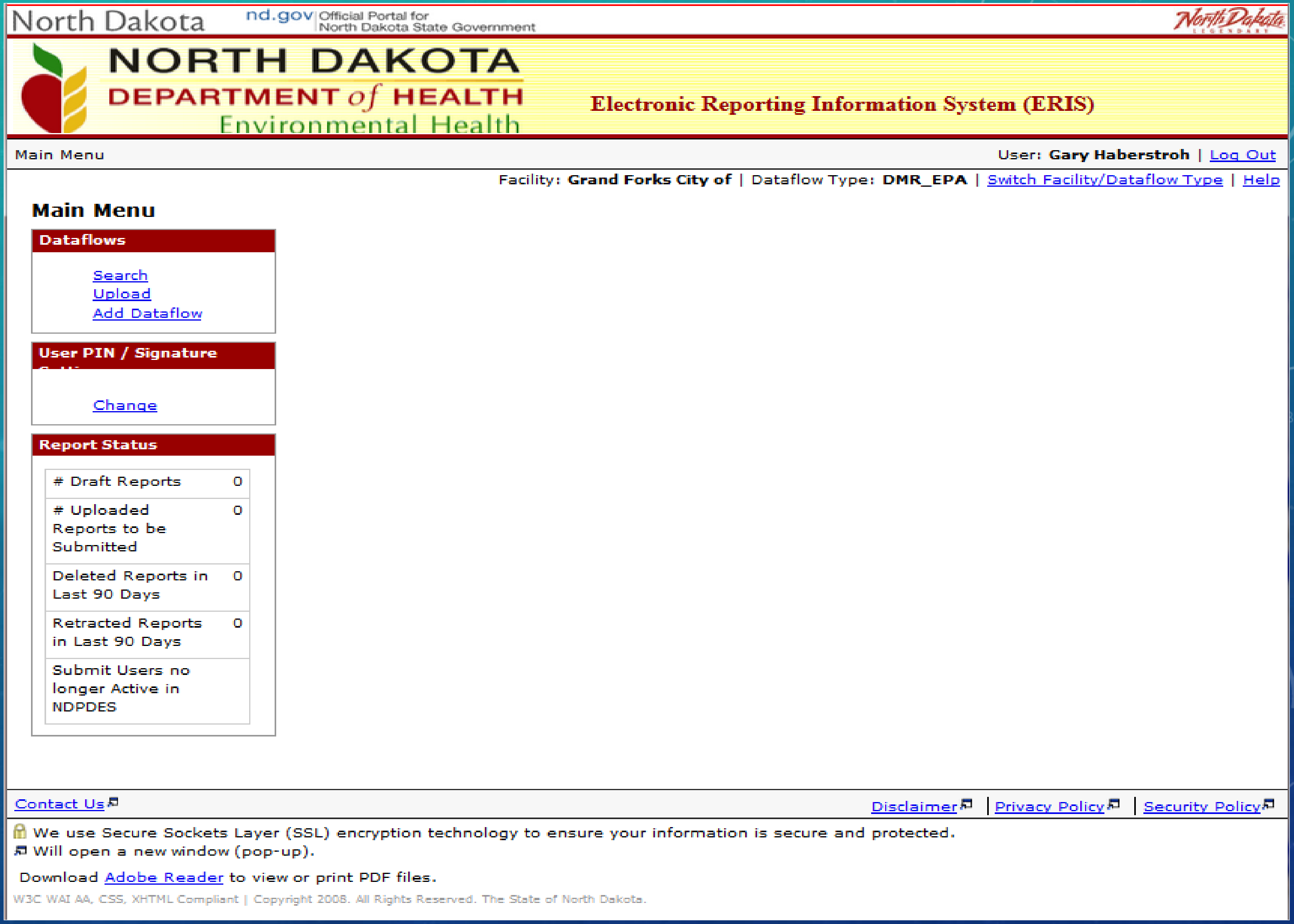
The ability for industry to authenticate once and seamlessly traverse to others states is appealing to Wyoming as it provides a better user experience for our industry users.

PARTNER EXPERIENCE

Rheanna Kautzman and Gary Haberstroh
ND Department of Health

NORTH DAKOTA EXPERIENCE

- Background on ERIS
- ISOL Project Experience
- Future Plans for this functionality in ND



North Dakota nd.gov Official Portal for North Dakota State Government

NORTH DAKOTA DEPARTMENT of HEALTH Environmental Health

Electronic Reporting Information System (ERIS)

Main Menu

User: **Gary Haberstroh** | Log Out

Facility: **Grand Forks City of** | Dataflow Type: **DMR_EPA** | Switch Facility/Dataflow Type | Help

Main Menu

Dataflows

Search
Upload
Add Dataflow

User PIN / Signature

Change

Report Status

# Draft Reports	0
# Uploaded Reports to be Submitted	0
Deleted Reports in Last 90 Days	0
Retracted Reports in Last 90 Days	0
Submit Users no longer Active in NDPDES	

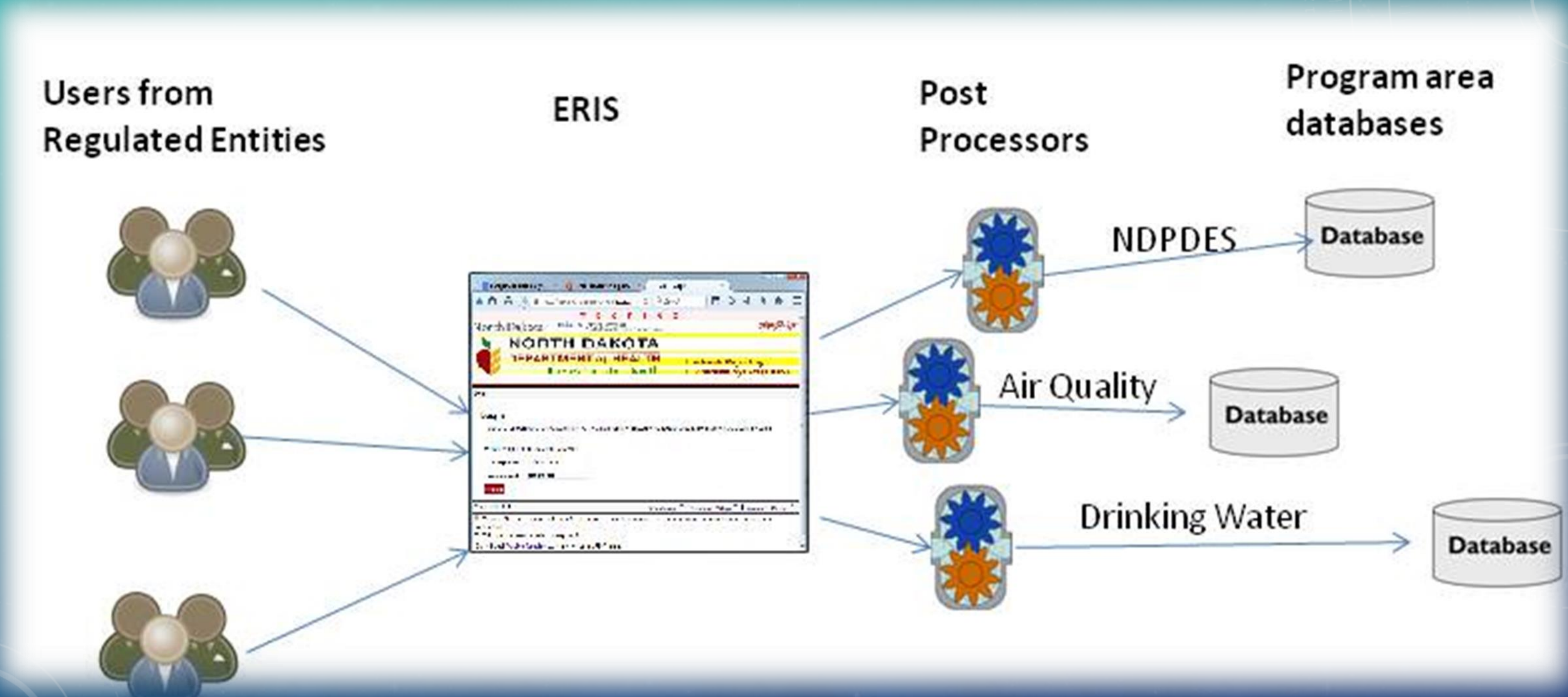
Contact Us | Disclaimer | Privacy Policy | Security Policy

We use Secure Sockets Layer (SSL) encryption technology to ensure your information is secure and protected.
Will open a new window (pop-up).

Download Adobe Reader to view or print PDF files.

W3C WAI AA, CSS, XHTML Compliant | Copyright 2008. All Rights Reserved. The State of North Dakota.

SINGLE POINT FOR ELECTRONIC REPORTING



EXPERIENCE ON THIS PROJECT

- Federated ID was done with configuration settings only
- Special coding was not required to enable federated ID

FUTURE PLANS - ND ENVIRONMENTAL PORTAL

- Make public user interface for non registered user
- Allow users to view and download public data
- Submit records requests
- Submit applications
- Submit complaints

- Enable Department staff to see regulated entity info from other states
- Be able to tie into EPA Portal concept

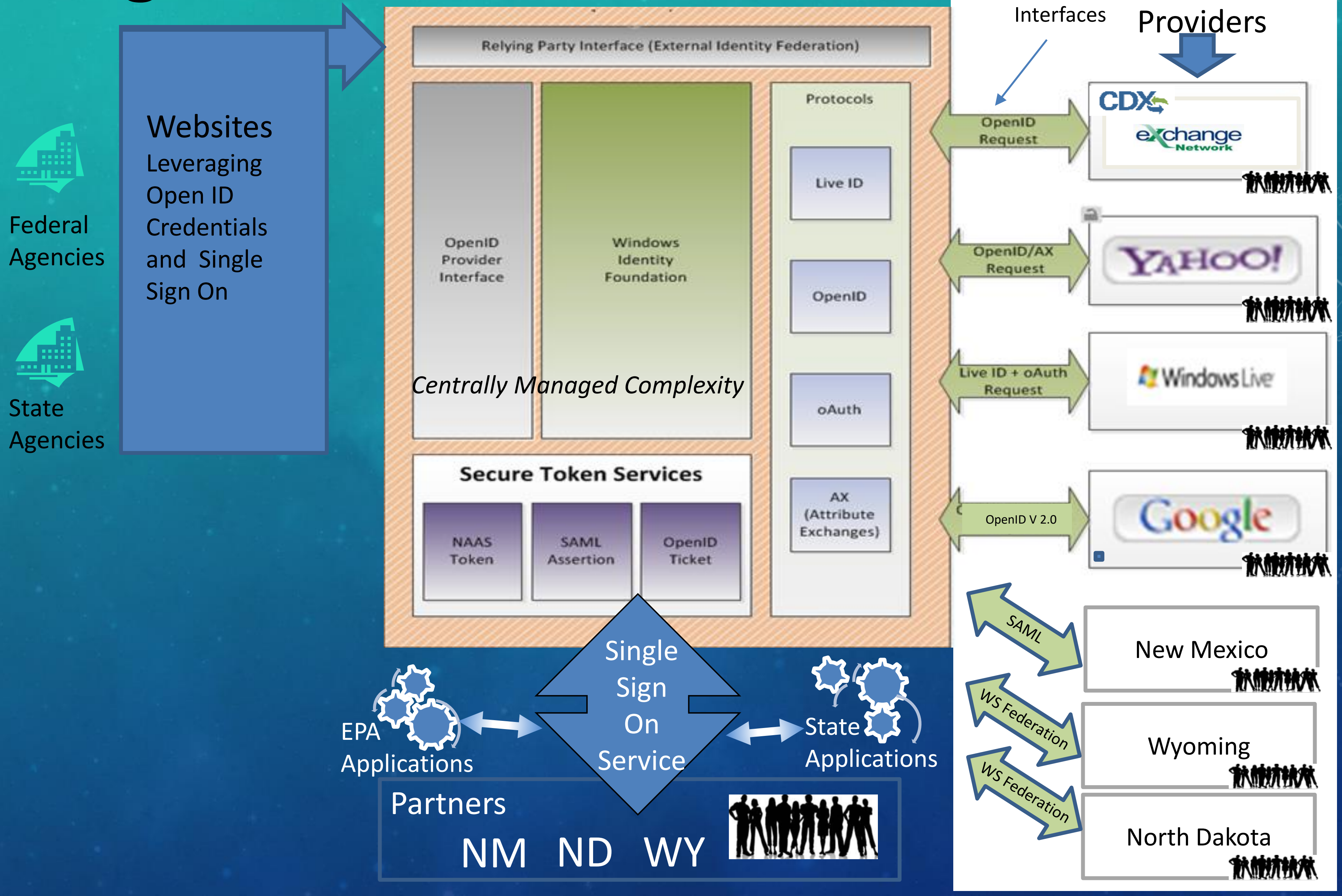
PARTNER EXPERIENCE

Chris Clark
EPA OEI

BRIDGE BACKGROUND

- Creates a trust framework between partner identity management systems for authentication
- Supports services for single sign-on across the enterprise
- 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

Bridge Architecture



Federal Agencies

State Agencies

Websites Leveraging Open ID Credentials and Single Sign On

Relying Party Interface (External Identity Federation)

OpenID Provider Interface

Windows Identity Foundation

Centrally Managed Complexity

Secure Token Services

NAAS Token

SAML Assertion

OpenID Ticket

Protocols

Live ID

OpenID

oAuth

AX (Attribute Exchanges)

Provider specific Interfaces

Identity Providers

OpenID Request

OpenID/AX Request

Live ID + oAuth Request

OpenID V 2.0

SAML

WS Federation

WS Federation

New Mexico

Wyoming

North Dakota

Single Sign On Service

EPA Applications

State Applications

Partners

NM ND WY

BRIDGE COMPONENTS

- *Identity Federation Multi-Protocol Processor:* Supports various security protocols such as OpenID, oAuth, Attribute Exchanges (AX) and 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
- *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
- *EN OpenID Provider:* 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 and which are enforced during token validation

ENHANCEMENTS

- WS-Federation Interface for relying party integration and single sign on
  - an Identity Federation specification, developed by a group of companies
- Second factor authentication support
  - "multi **factor authentication**" that requires not only a password and username but also something that only, and only, that user has on them
- Support for Azure Active Directory
  - multi-tenant service from Microsoft that offers identity and access capabilities for applications
- Support for Shibboleth
  - allows people to sign in using just one identity to various systems run by federations of different organizations or institutions based on Security Assertion Markup Language (SAML)
- Support for Personal Identity Validation (PIV) cards
  - Cards used to grant Federal facilities and information systems access for all applicable Federal applications
- Documentation for state integrators

IDENTITY MANAGEMENT PROJECT

- How it went
  - The Bridge integrations went smoothly with NM, WY and ND
- What were some of the positive things
  - The project was well organized
  - Integrators were successful with both Identity providers (IdP) and RP
- Did we have any lessons learned
  - Social Media IdPs can change without warning
  - Integrating both IdP and Relying Party was easier than anticipated
- Recommendations for the future
  - Evaluate alternative traversal methods
  - Tune documentation to minimize burden for adopters

PARTNER EXPERIENCE

Mary Montoya
NM Environment Department

PROJECT DELIVERABLES

✓ Discovery & Analysis Documents

- Discovery Sessions: Summaries & Details – EPA, NM, WY, ND
- Gap Analysis Documents – NM, WY, ND

✓ Gap Analysis Documents

- Use Cases & Analysis – NM, WY, ND

✓ Identity Management Industry Research & Analysis

- Industry Survey, Analyses, & Comparisons

✓ Presentations & Demonstrations

- Partner IdM, ISOL Project, & Proof of Concept

✓ Developer's Guides & Code Samples

- Java, PHP, C# .NET, VB .NET
- IdP, RP Originating, RP Traversal

ISOL TECHNICAL RECOMMENDATIONS

- ❖ Identity Provider (IdP)
  - Choose Standalone, Technology-Appropriate, Well-Supported Open Source Products
    - More flexible • Little or no coding • Choices for Identity Store: AD, LDAP, DB, or WS
    - OpenID Connect (OIDC) Protocol preferred for future IdP applicability to mobile apps
    - Examples: IdentityServer (C# .NET), phpOIDC (PHP), Gluu (Java), …
- ❖ Relying Party (RP)
  - Web Apps Use Passive Authentication with Identity Bridge (WS-Federation)
    - Less RP programming for traversal • User-friendly SSO • Simple links & bookmarks
  - WS-Federation – Choose technology-appropriate, well-supported open source libraries
    - Examples: Microsoft WIF (.NET built-in), Apache CXF Fediz (Java), SimpleSAMLphp (PHP)
  - SAML – Choose technology-appropriate, well-supported open source libraries
    - Examples: SimpleSAMLphp (PHP), OpenSAML (Java), Spring Security (Java), WIF (.NET built-in)
- ❖ Identity Bridge
  - Implement New Passive Validation Endpoint that Returns Login Status to Relying Party
  - Revise Documentation per These Recommendations & Extend to Non-Microsoft Platforms

ISOL GOVERNANCE RECOMMENDATIONS

- Identity Provider (IdP)
  - All Partners Standardize the Set of Identity Claims per Mutual Agreement
  - Add Claim for Level of Assurance (LOA) per Partner Agreements
  - Add Yes/No Claim for CROMERR-Compliance per Partner Agreements
  - Use Identity Bridge’s Claim-Mapping Feature to Standardize External IdP Claims
    - i.e.: Map Identity Claims from Facebook, Google, Yahoo, … to the Agreed Standard Claims
  - Design These Standards to Reduce Burden on Partner IdPs
- Relying Party (RP)
  - Use the Standardized Set of Identity Claims per Partner Agreements
  - Develop Partner Agreement to Handle Authorization in an Appropriate Standard Way per the Identity Claims of LOA and CROMERR-Compliance
- Identity Bridge
  - Add Appropriately Low LOA Claim for External IdPs (Facebook, Google, …)
  - Add CROMERR-Compliance Claim for External IdPs – Always with Value of “No”

BEYOND SCOPE, NEXT STEPS & CONCLUSIONS

- Operations & Support
- Governance & Policies
- CROMERR Integration
- Partner Adoption Engagements
- How and Why Does This Make Things Better?
- What’s Next?

The ISOL Project Team

NM	Mary Montoya	MaryH.Montoya@state.nm.us
	Charlie Fitch	Charles.Fitch@state.nm.us
	Ullas Joseph	Ullas.Joseph@state.nm.us
	Dan Gandhi	Dan.Gandhi@state.nm.us
	Mark Morell	Mark.Morell@state.nm.us
	Bogi Malecki	
	Tom McMichael	
	Sam Jenkins	
	Ellen Rabin	
EPA	Connie Dwyer	Dwyer.Connie@epa.gov
	Chris Clark	Clark.Chris@epa.gov
	Yunhao Zhang	yzhang2006@gmail.com
	Lucas Gentry	lucas.gentry@cgifederal.com
	Zerihun Tegegn	zerihun.tegegn@cgifederal.com
WY	Steven Girt	steve.girt@wyo.gov
	Ryan Fagan	ryan@gannettpeaktech.com
	Anthony DeMillard	tony@gannetpeaktech.com
	Heather Kenworthy	
ND	Gary Haberstroh	ghaberst@nd.gov
	Luka Radunovic	lradunovic@nd.gov
	Rheanna Kautzman	rKautzman@nd.gov