E-Enterprise Shared Identity Management Concept of Operations

Version 1.00

June 24, 2015

Table of Contents

List of Exhibits

Revision Log

Date	Version No.	Description	Author
May 27, 2015	0.01	Delivery of Draft E-Enterprise Shared Identity Management Concept of Operations	Luke Gentry, CGI Federal
June 24, 2015	1.00	Delivery of Final E-Enterprise Shared Identity Management Concept of Operations	Luke Gentry, CGI Federal

Acknowledgements

The E-Enterprise Shared Identity Management Work Group team developed this Concept of Operations with the support and contributions of a number of individuals and programs within EPA, ECOS, and state agencies. The work group acknowledges:

State and EPA E-Enterprise Shared Identity Management Work Group	
Connie Dwyer, EPA OEI, Co-Chair	Steve Girt, WY DEQ, Co-Chair
Kimberly Hoke, MO DNR	Chris Clark, EPA
Dalroy Ward, EPA	Elisa Willard, CO DPHE
Eric Cleckler, AL DEM	Joe Carioti, EPA
Jurgen Koch, TX CEQ	Martin Husk, EPA
Sam Jenkins, NM ED	Tom Gaskill, Maricopa County
Thomas Waller, OH EPA	Tobias Schroeder, EPA
Tom McMichael, NM ED	Ken Blumberg, EPA
Philip Omaoeng, NM ED	Vince Allen, EPA
Other Contributors:	
Kurt Rakouskas, Exchange Network	Mary Montoya, NM ED
Rob Willis, Ross Strategic	Jimmy Mahaday, Ross Strategic
Lucas Gentry, CGI Federal	Beth Graves, ECOS
Peter Soyka, E-Enterprise Coordinator	Jason Payne, CGI Federal
Greg McNelly, ECOS	Chuck Freeman, EPA
Greg Mitchell, EPA	Walter Baucom, CGI Federal

1 Introduction

1.1 E-Enterprise for the Environment

E-Enterprise for the Environment is an initiative that will transform the business and delivery of environmental protection in the United States. Through the collaboration of the states, EPA, and tribes, E-Enterprise will improve environmental performance and enhance services to the regulated community, environmental agencies, and the public. The primary purpose of E-Enterprise is to improve environmental protection.

EPA and the states have worked together through the State-EPA E-Enterprise Working Group to create the vision for E-Enterprise. The first step in defining E-Enterprise was the creation of a Conceptual Blueprint that defines the design and operating principles as well as six primary E-Enterprise Components.

1.1.1 E-Enterprise Design and Operating Principles

The ten principles identified in the Blueprint are a combination of assertions about the operation of E-Enterprise and assumptions regarding system capabilities.

1. Partnership of Environmental Government Regulators
2. Honoring Delegated Authority
3. Modernize and Improve Environmental Regulations and Programs, and their Implementation
4. Joint Governance Prioritizing Activities
5. Emphasizing User Perspective
6. Creating and Expanding Systems to Improve Two-way Business Transactions
7. Interoperability of Partner Systems and Partner Use of EPA Systems
8. Open Data and Web Services
9. Advanced Monitoring Technologies and New Data Collection and Analysis Techniques
10. Shared Technical and Programmatic Infrastructure

See Section 3 of the Blueprint for additional content and context regarding these principles.

1.1.2 E-Enterprise Components

The Blueprint identified six primary components that will make up E-Enterprise.

1. Modernizing and Streamlining Programs and Regulations
2. Portfolio of Advanced Monitoring Technologies
3. The E-Enterprise Portal
4. Partner Access and Transaction Systems
5. Open Data and Web Services
6. E-Enterprise Shared Technical and Programmatic Infrastructure

See Section 4 of the Blueprint for additional content and context regarding these components.

1.1.3 Governance and Coordination

The E-Enterprise Leadership Council (EELC) was formed to provide coordination and oversight for E-Enterprise activities. In cooperation with the EELC, the Exchange Network Leadership Council (ENLC) supports information technology projects of E-Enterprise. The ENLC formed the E-Enterprise Architecture Integrated Project Team as a means to produce a subset of the deliverables identified by the Blueprint that will move the E-Enterprise effort forward. The E-Enterprise Shared Identity Management System Scoping Work Group is a work group under the E-Enterprise Architecture Integrated Project Team formed to provide stakeholder input into the design and development of the E-Enterprise Shared Identity Management System (EIDMS).

1.2 E-Enterprise Shared Identity Management

Among its goals, E-Enterprise envisions a seamless and secure network of services and systems to improve two-way business transactions between the regulated community and environmental government regulators (Design and Operating Principle #7). One critical underpinning of that vision is an interoperable system for effectively sharing user identities and credentials across different levels of government. A Shared Identity Management System will establish a trust framework that will allow EPA, states, tribes, and local governments to share identity credentials and allow their customers to use their username and password across applications and participating partner portals. This can include state, tribal, and local government portals re-using EPA-issued credentials, and also EPA re-using state, tribal, and local government issued credentials.

1.3 Approach

Under the auspices of the E-Enterprise Architecture Integrated Project Team (IPT) and using the E-E Architectural Principles as guidance, the E-Enterprise Shared Identity Management System Scoping Work Group brought together E-Enterprise partners from EPA, states, and local governments. The work group conducted scoping for the E-Enterprise Shared Identity Management System focusing on identifying collective use cases, requirements, and overall functionality documented in this Concept of Operations that will also serve to inform the next steps in development of an identity management solution.

1.3.1 Work Group Activities

In order to achieve the primary objective of gathering input and requirements from EPA, state, and local government stakeholders for an identity management solution, the group engaged in the following activities:

- Discussed general properties and models of federated identity management
- Discussed current research on possible approaches for E-Enterprise Shared Identity Management

- Discussed policy and governance issues regarding E-Enterprise Shared Identity Management
- Gathered information and lessons learned from current, previous, or planned identity management initiatives at the federal, state, or local level
- Identified use cases for the E-Enterprise Shared Identity Management System
- Gathered and documented partner business, functional, and technical requirements for the E-Enterprise Shared Identity Management System

1.3.2 Scope of Document

The primary objective of this work group is to gather input and requirements from EPA, state, and local government stakeholders that will support the scoping and development of the EIDMS. The purpose of this document is to capture the information gathered by the work group and to provide a foundation from which subsequent phases of work can be built upon. Subsequent phases may include:

- Documenting potential solution alternatives
- Identifying any critical partner administrative procedural requirements needed to support the workflows identified in the Concept of Operations
- Proposing an implementation plan for a pilot that will demonstrate successful integration with the system by multiple partner agencies

The scope of this document includes the following primary components:

- Critical use cases for shared identity management (including interaction of identity store options with EPA national systems, E-Enterprise portal, and state/tribal/local systems)
- Partner business, functional, and technical requirements
- Governance areas that will have to be defined and agreed upon by participating partners
- A description of the system’s desired functionality

2 References

- E-Enterprise for the Environment Conceptual Blueprint: Principles and Components
  http://www.exchangenetwork.net/ee/EEnterprise_Conceptual_Blueprint_013114.pdf
- Environmental Information Exchange Network E-Enterprise for the Environment
  http://www.exchangenetwork.net/e-enterprise/
- EPA E-Enterprise for the Environment
  http://www2.epa.gov/e-enterprise
- EPA Leadership of E-Enterprise for the Environment
  http://www2.epa.gov/e-enterprise/leadership-e-enterprise-environment#Joint Governance
- [id]MANAGEMENT.GOV
  http://www.idmanagement.gov/
- National Science and Technology Council Identity Management Task Force Report
  http://www.biometrics.gov/Documents/IdMReport_22SEP08_Final.pdf
- National Institute of Standards and Technology Electronic Authentication Guideline
  http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
- Charter for State and EPA E-Enterprise Leadership Council
  http://www.exchangenetwork.net/wp-content/uploads/2014/03/09-16-13-Signed-EELC-Charter.pdf
- E-Authentication Guidance for Federal Agencies Memorandum (M-04-04)
  https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

3 Purpose

The importance of including an E-Enterprise Shared Identity Management System as part of the E-Enterprise Shared Technical and Programmatic Infrastructure was identified explicitly by the State-EPA E-Enterprise Working Group's Blueprint Team as a method to support Design and Operating Principle #7 (Interoperability of Partner Systems and Partner Use of EPA Systems).

The Blueprint defines this principle as:

> *E-Enterprise is envisioned to evolve the operation of partner's systems toward a set of common functional goals, consistent with their respective needs and ability to implement changes in their systems or approaches. Many partners will continue to operate their own systems. E-Enterprise investments will be designed to be interoperable, to the extent possible, with these systems to provide a seamless user experience. States will evaluate if EPA-provided systems and services can replace separate existing systems, especially as those systems reach the end of their lifecycles. E-Enterprise will also provide a forum through which states and EPA can learn from and potentially adopt proven state solutions.*

The role of identity management in supporting this principle has been consistently reinforced in the Blueprint and subsequent E-Enterprise planning. In further expanding on Principle #7 the Blueprint goes on to say that, "…evolving toward a federated identity system which will allow users to re-use credentials between EPA program applications and state applications is a key example of this integration objective.". The Blueprint Team identified this Concept of Operations document as a foundational technical document related to E-Enterprise Component #6, Shared Programmatic and Technical Infrastructure.

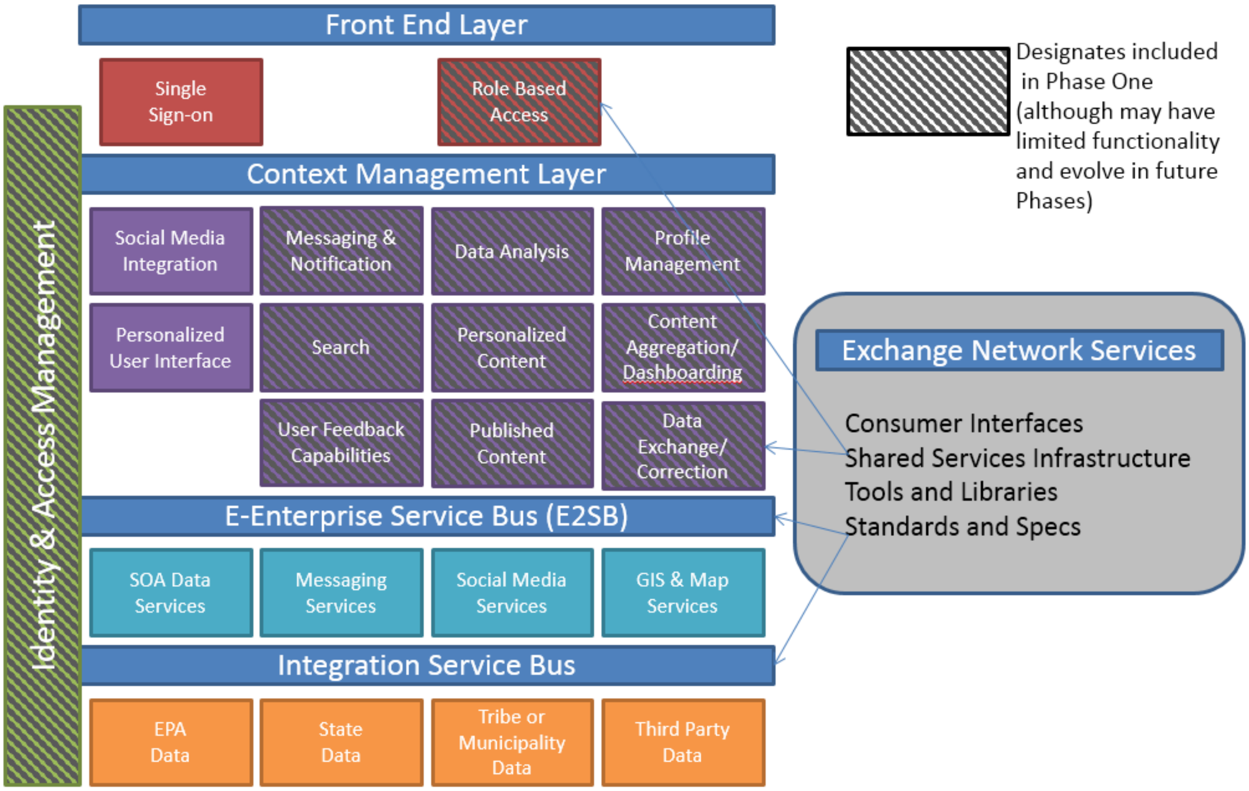
3.1 Identity Management and the E-Enterprise Portal

Improvement of the quality of services delivered to the public and the regulated community and an emphasis on user experience are recurring themes in the underlying principles and goals and objectives of E-Enterprise. The E-Enterprise Portal is a central component (Component #3) in the E-Enterprise vision and will be instrumental in providing users with quality services and a positive user experience. The Portal will provide an enterprise-level view to the public and regulated community. This view will be user customizable and be a key point of integration across partners in the enterprise.

The Portal seeks to provide a seamless experience for users through the integration with partner portals and applications. A seamless user experience across multiple portals and applications will require partners to share the identity of users between portals and applications. The EIDMS will facilitate this key aspect of the E-Enterprise Portal architecture. Not only will the system be integral in providing interoperability and a seamless user experience, but it will also support other aspects of the Portal that are closely tied to the concept of identity, such as social media integration, personalization, messaging, and profile management. The E-Enterprise Portal Conceptual Architecture (Exhibit 3-1) developed by the E-Enterprise Architecture Integrated

Project Team[1] demonstrates the critical supporting role that "Identity and Access Management" play in the overall Portal architecture.

Exhibit 3-1 E-Enterprise Portal Conceptual Architecture



3.2 Goals and Objections

The concept of identity management in the digital context has existed for as long as systems and applications have contained the concept of distinct users. The 2008 National Science and Technology Council Identity Management Task Force Report defined Identity Management as:

> *The combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguarding of personal identity information. The primary goal of the Identity Management process is to assign attributes to a digital identity and to connect that identity to an individual.*

Traditionally, the management of digital identities has been handled by individual applications. These stand-alone identity stores are also known as "identity silos" and they have proliferated over time. Identity management solutions were created to accommodate the use of a single identity for a user across multiple systems within the same network or domain. These solutions are referred to as centralized identity management solutions.

[1] The E-Enterprise Architecture Integrated Project Team is running in parallel with the E-Enterprise Shared Identity Management System Scoping Work Group and the official graphic related to Exhibit 3-1 may change in their final work products.

Many factors have contributed to an increase in the need for users to access systems outside of their network or domain, and for systems and applications to provide access to external users. Identity silos and centralized, or domain-specific, identities impose a burden on users who must register with individual applications as well as on application owners who must duplicate user registration processes and functionality across systems. In addition to the burden related to duplicative registration, individual or stand-alone identity management can result in significant challenges for integrating systems.

E-Enterprise actively seeks to build a network of sorts from multiple domains and applications. Each state, EPA, tribe, or local government portal or application that may be integrated in some fashion through E-Enterprise creates the potential for cross-domain user and identity interaction. The very nature of the regulatory processes and aggregation of environmental data that E-Enterprise seeks to support introduces both the need and desire for users to access portals, systems, or services from providers representing multiple domains participating in E-Enterprise.

The challenges created by this increasingly common scenario of cross-domain user access are common challenges within government and business. Enterprise identity management (EIdM), most commonly known now as “federated identity management” is the evolving approach for managing these challenges. At its most basic definition, enterprise identity management is an approach for managing identities and access to systems and services that cross security domains.

The long-term vision of E-Enterprise involves the integration of systems and services from a wide variety of participating organizations including states, EPA, tribes, and local government. For the most part, the current landscape of state, EPA, tribal and local portals and systems maintain their own user identity information resulting in redundant user administration functions for application owners and a burden on users who are forced to maintain multiple digital identities.

An Enterprise Shared Identity Management System will support multiple E-Enterprise Design and Operating Principles, including:

- Principle #5: Emphasizing User Perspective
- Principle # 6: Creating and Expanding Systems to Improve Two-way Business Transactions
- Principle #7: Interoperability of Partner Systems and Partner Use of EPA Systems
- Principle #8: Open Data and Web Services
- Principle #10: Shared Technical and Programmatic Infrastructure

In addition, an Enterprise Shared Identity Management System will play an important role in several of the six components of E-Enterprise, including:

- Component #3: E-Enterprise Portal
- Component #4: Partner Access and Transaction Systems
- Component #5: E-Enterprise Open Data and Web Services
- Component #6: E-Enterprise Shared Technical and Programmatic Infrastructure

The primary benefits of enterprise identity management include:

- Enabling users of one domain to securely access systems and services of another domain
- Eliminating the need for redundant user administration, resulting in:

  - Reduced cost to partners who may no longer need to develop and maintain user registration
  - Reduced burden to users and improve the experience for end-users who no longer need to register and maintain identity information in multiple systems
- Creating an infrastructure that will allow for interoperability and a seamless user experience between partner systems and services
- Providing single sign-on and sign-off capabilities across partner systems and services

4 Concept for Proposed Solution

The proposed features and conceptual architecture of the E-Enterprise Shared Identity Management System are a result of work group efforts to compile critical use cases, business and functional requirements, technical requirements, and governance and policy needs.

4.1 Critical Use Cases

The work group collaboratively identified the critical use cases for the EIDMS that are described in this section. This list identifies the critical, high-level use cases that must be supported by the system in order to support the current expectations of E-Enterprise. As E-Enterprise use cases are identified or modified, EIDMS use cases may also be added or modified.

Exhibit 4-1 Critical Use Cases

Number	Title	Description
UC1	Web-based access to EPA system (Using a state, tribe, or local government issued identity (approved identity provider (AIP))	A user seeks to access an EPA system (the relying party) using an identity issued by a state, tribe, or local government system (the identity provider)
UC2	Web-based access to state, tribe, or local government system (Using an EPA issued identity (AIP))	A user seeks to access a state, tribe, or local government system (the relying party) using an identity issued by an EPA system (the identity provider)
UC3	Web-based access to state, tribe, or local government system (Using an identity issued by a non-EPA partner (AIP))	A user seeks to access a state, tribe, or local government system (the relying party) using an identity issued by a partner State system (the identity provider)
UC4	Web service access to EPA service (Using a state, tribe, or local government issued identity (AIP))	A user action or scheduled process seeks to access an EPA system service (a web service, for example) that does not involve a redirect to the relying party (the EPA system)
UC5	Web service access to a state, tribe, or local government service (Using an EPA issued identity (AIP))	A user action or scheduled process seeks to access a state, tribe, or local government system service (a web service, for example) that does not involve a redirect to the relying party (the state system)
UC6	Web service access to a state, tribe, or local government service (Using an identity issued by a non-EPA partner (AIP))	A user action or scheduled process seeks to access a state, tribe, or local government system service (a web service, for example) that does not involve a redirect to the relying party (the partner state system)
UC7	Authorization/role management	A user accesses a system (the relying party) authenticating with an identity provided by another system (the identity provider) and requests authorization from the relying party to perform a specific action within the relying party
UC8	User attribute exchange	A user accesses a system (the relying party) authenticating with an identity provided by another system (the identity provider) and the relying party requests specific attributes be provided by the identity provider
UC9	Enforcing Level of Assurance (LOA)	A user accesses a system (the relying party) authenticating with an **approved** identity provided by another system (the identity provider) where the identity provider assigned level of assurance is lower than that required by the relying party

UC10	A regulated user’s account has been disabled by one or more partners	A user’s account has been disabled by a participating partner and notification is provided to other identity providers with a specific disposition recommendation to the user’s IDP
UC11	A partner’s authentication security system has been compromised	An identity provider within the system has potentially been compromised and must be disabled

4.1.1 Web-based access to EPA system (Using a state, tribe, or local government issued identity)

One of the fundamental goals and benefits of an enterprise identity management system is allowing a user to access systems across the various domains that are part of the enterprise using a single, shared identity. This use case addresses the use of a federated identity for access to a web application provided within the context of E-Enterprise.

4.1.1.1 Description of Service

Allow a user to access an EPA system or portal (the relying party) using an identity issued by a state, tribe, or local government system (the identity provider).

1. User attempts to access a protected resource at an EPA system or portal (the relying party).
2. User is offered a choice of identity providers.
3. User chooses a state, tribe, or local government identity provider.
4. User is redirected to the selected identity provider.
5. User is authenticated by the identity provider after providing credential information at the identity provider login page.
6. User is redirected to the EPA system or portal.
7. EPA system or portal successfully validates the authentication and allows access if the user is authorized to use the application (by the relying party) and if the identity is from an identity provider of an appropriate assurance level.

4.1.2 Web-based access to state, tribe, or local government system (Using an EPA issued identity)

One of the fundamental goals and benefits of an enterprise identity management system is allowing a user to access systems across the various domains that are part of the enterprise using a single, shared identity. This use case addresses the use of a federated identity for access to a web application provided within the context of E-Enterprise.

4.1.2.1 Description of Service

Allow a user to access a state, tribe, or local government system (the relying party) using an identity issued by an EPA system (the identity provider).

1. User attempts to access a protected resource at a state, tribe, or local government system (the relying party).
2. User is offered a choice of identity providers.
3. User chooses an EPA identity provider.
4. User is redirected to the selected identity provider.
5. User is authenticated by the identity provider after providing credential information at the identity provider login page.
6. User is redirected to the state, tribe, or local government system.
7. The state, tribe, or local government system validates the authentication and allows access if the user is authorized to use the application (by the relying party) and if the identity is from an identity provider of an appropriate assurance level.

4.1.3 Web-based access to state, tribe, or local government system (Using an identity issued by a non-EPA partner)

One of the fundamental goals and benefits of an enterprise identity management system is allowing a user to access systems across the various domains that are part of the enterprise using a single, shared identity. This use case addresses the use of a federated identity for access to a web application provided within the context of E-Enterprise.

4.1.3.1 Description of Service

Allow a user to access a state, tribe, or local government system (the relying party) using an identity issued by another state, tribe, or local government system (the identity provider).

1. User attempts to access a protected resource at a state, tribe, or local government system (the relying party).
2. User is offered a choice of identity providers.
3. User chooses a state, tribe, or local government identity provider.
4. User is redirected to the selected identity provider.
5. User is authenticated by the identity provider after providing credential information at the identity provider login page.
6. User is redirected to the relying party state, tribe, or local government system.
7. The relying party state, tribe, or local government system validates the authentication and allows access if the user is authorized to use the application (by the relying party) and if the identity is from an identity provider of an appropriate assurance level.

4.1.4 Web service access to EPA service (Using a state, tribe, or local government issued identity)

One of the fundamental goals and benefits of an enterprise identity management system is allowing a user to access systems across the various domains that are part of the enterprise using a single, shared identity. This use case addresses the use of a federated identity for access to a web service provided within the context of E-Enterprise.

4.1.4.1 Description of Service

Allow a user action or scheduled process to access an EPA system service (a web service, for example) using a state, tribe, or local government issued identity that does not involve a redirect to the relying party (the EPA system). For example, E-Enterprise may evolve to allow for the display of a unified user To-Do List within multiple partner systems or portals. An aggregated To-Do List could conceivably be implemented as a series of web services made available in multiple partner systems.

1. An authenticated user using a state, tribe, or local government issued identity attempts to access a protected EPA service from within a partner system.
2. The state, tribe, or local government system issues a service call providing identity information and proof of authentication.
3. The EPA web service validates the authentication information and performs any applicable authorization checks and returns the requested response if the authorization is valid and the user is authorized to receive the requested information.
4. The state, tribe, or local government system receives and processes the response.

4.1.5 Web service access to a state, tribe, or local government service (Using an EPA issued identity)

One of the fundamental goals and benefits of an enterprise identity management system is allowing a user to access systems across the various domains that are part of the enterprise using a single, shared identity. This use case addresses the use of a federated identity for access to a web service provided within the context of E-Enterprise.

4.1.5.1 Description of Service

Allow a user action or scheduled process to access a state, tribe, or local government service (a web service, for example) using an EPA issued identity that does not involve a redirect to the relying party (the state, tribe, or local government system). For example, E-Enterprise may evolve to allow for the display of a unified user To-Do List within multiple partner systems or portals. An aggregated To-Do List could conceivably be implemented as a series of web services made available in multiple partner systems.

1. An authenticated user using an EPA issued identity attempts to access a protected state, tribe, or local government system service from within a partner system.
2. The partner system issues a service call providing identity information and proof of authentication.
3. The state, tribe, or local government web service validates the authentication information and performs any applicable authorization checks and returns the requested response if the authorization is valid and the user is authorized to receive the requested information.

4. The partner system receives and processes the response.

4.1.6 Web service access to a state, tribe, or local government service (Using an identity issued by a non-EPA partner)

One of the fundamental goals and benefits of an enterprise identity management system is allowing a user to access systems across the various domains that are part of the enterprise using a single, shared identity. This use case addresses the use of a federated identity for access to a web service provided within the context of E-Enterprise.

4.1.6.1 Description of Service

Allow a user action or scheduled process to access a state, tribe, or local government service (a web service, for example) using an identity issued by another state, tribe, or local government that does not involve a redirect to the relying party (the state, tribe, or local government system). For example, E-Enterprise may evolve to allow for the display of a unified user To-Do List within multiple partner systems or portals. An aggregated To-Do List could conceivably be implemented as a series of web services made available in multiple partner systems.

1. An authenticated user using a state, tribe, or local government issued identity attempts to access a protected state, tribe, or local government system service from within a partner system.
2. The partner system issues a service call providing identity information and proof of authentication.
3. The state, tribe, or local government web service validates the authentication information and performs any applicable authorization checks and returns the requested response if the authorization is valid and the user is authorized to receive the requested information.
4. The partner system receives and processes the response.

4.1.7 Authorization/role management

Authentication and authorization are important concepts in enterprise identity management. Authentication is the act or process of determining that a person or user is who they claim to be. Within enterprise identity management, authentication is the responsibility of the identity provider. Authorization is the act or process of determining which permissions or roles that a user has within a system. Within enterprise identity management, authorization is the responsibility of the relying party.

4.1.7.1 Description of Service

Determine whether or not a user is authorized to perform a specific action after they have been authenticated.

1. User attempts to access a protected resource at a partner system or service (the relying party).
2. User is offered a choice of identity providers.

3. User chooses an identity provider.
4. User is redirected to the selected identity provider.
5. User is authenticated by the identity provider after providing credential information at the identity provider login page.
6. User is redirected back to the relying party system or service.
7. The relying party system or service validates the authentication.
8. The relying party system or service performs its internal processes to determine if the user has access to the system and the permissions appropriate to perform the requested action (authorization).

4.1.8 User attribute exchange

Within the federated model of enterprise identity management, some of the authoritative user attribute data for a given identity will reside with the identity provider that the user chooses to use for participation in E-Enterprise systems and services. The EIDMS will support the exchange of attributes from an identity provider to the relying party when the identity provider supplies a positive assertion in response to an authentication/login request. A common set of attributes that can be exchanged within the enterprise will be defined. Participating organizations may choose to perform an “extended” registration within their relying party systems to capture additional information from the user.

4.1.8.1 Description of Service

Consume user attributes exchanged within the enterprise between an identity provider and a relying party.

1. User attempts to access a protected resource within the enterprise.
2. User is offered a choice of identity providers.
3. User chooses an identity provider.
4. User is redirected to the selected identity provider.
5. User is authenticated by the identity provider after providing credential information at the identity provider login page.
6. User is redirected back to the relying party with an assertion of authentication and authoritative user attribute data from the identity provider.
7. The relying party validates the authentication.
8. The relying party performs its internal processes to determine if the user has access to the system and the permissions appropriate to perform the requested action.
9. The relying party extracts the supplied user attribute data and uses it within the relying party system as desired.

4.1.9 Enforcing Level of Assurance (LOA)

E-authentication is an important concept in enterprise identity management. In their 2013 Electronic Authentication Guideline, The National Institute of Standards and Technology defined e-authentication as, “…the process of establishing confidence in user identities electronically presented to an information system.” Identity providers in an enterprise are assigned one of four standard levels of assurance (LOA) ranging from providing little or no confidence in the validity of an identity to very high confidence in identity validity. Relying parties are responsible for enforcing that a user is using an identity that provides a high enough LOA to perform requested functionality.

4.1.9.1 Description of Service

Manage an occurrence of a user accessing a system (the relying party) authenticating with an identity provided by another system (the identity provider) where the identity provider assigned LOA is lower than that required for the action that they are attempting to perform within the relying party.

1. User attempts to access a protected resource within the enterprise.
2. User is offered a choice of identity providers.
3. User chooses an identity provider.
4. User is redirected to the selected identity provider.
5. User is authenticated by the identity provider after providing credential information at the identity provider login page.
6. User is redirected back to the relying party with an assertion of authentication and authoritative user attribute data from the identity provider.
7. The relying party validates the authentication.
8. The relying party extracts the supplied user attribute data, including the identity provider’s assigned LOA.
9. The relying party determines that the action that the user is requesting requires a higher level of assurance than that supported by the user’s identity provider.
10. The relying party does not allow the user to perform the requested action.
11. In order for the user to perform the action, the user must re-authenticate with an identity provider that can provide the appropriate level of confidence in the user’s identity.

4.1.10 A regulated user’s account has been disabled by one or more partners

Enterprise identity management can serve to enhance security. When a user utilizes a single identity to interact with multiple partner organizations, enterprise identity management can help all participating organizations be aware of how a single identity is interacting across multiple domains. In some cases a partner organization may have cause to disable a user’s account because of security concerns.

4.1.10.1 Description of Service

Notify participating members of the EIDMS of the disabling of a user’s account.

1. Partner organization removes a user’s authorization in their system(s) (relying party).
2. The organization knows the identity provider and unique identifier associated with that identity that the user has utilized for access to their system(s).
3. The partner organization uses a central service of the enterprise to notify other participating organizations of the reason for disabling an account associated with an identity.
4. Other partner organizations receive the notification and act accordingly within their own system(s).
5. Optional – Identity is added to the Enterprise Reject List.

4.1.11 A partner’s authentication security system has been compromised

Enterprise identity management can serve to enhance security. Accepting identity information and authentication assurance from an external party introduces some risk to a relying party. Governance controls around identity provider level of assurance is one mechanism within enterprise identity management for mitigating risk. Notification services within the enterprise designed to alert participating members when a participating identity provider may be compromised can be another means of risk mitigation.

4.1.11.1 Description of Service

Notify participating members of the EIDMS when a participating identity provider has been compromised.

1. A participating identity provider suspects that their security has been compromised.
2. A central service is used to notify participating members of the possible security compromise of the participating identity provider.
3. The identity provider is disabled for utilization within the EIDMS.
4. Other partner organizations process and review usage within their systems of identities provided by the potentially compromised identity provider.

4.2 Key Business and Functional Requirements

The work group collaboratively identified the key business and functional requirements for the E-Enterprise Shared Identity Management System that are described in this section. This list is not comprehensive but seeks to identify the key, high-level requirements that must be supported by the system.

Exhibit 4-2 Business and Functional Requirements

Number	Description
F1	The Enterprise Identity Management Framework shall provide for the establishment of a framework of security trusts between the participating partners.
F2	The Enterprise Identity Management Framework shall establish a trust framework that EPA, states, tribes, and local governments can participate in.
F3	The Enterprise Identity Management solution shall provide a mechanism that allows EPA, states, tribes, and local governments to share identity credentials and allow their customers to use their username and password across partner applications, and in participating partner portals and other services.
F4	The Enterprise Identity Management Framework shall provide a mechanism that reduces user registration activities through the sharing of identity and reuse of user registration information.
F5	The Enterprise Identity Management Framework shall promote identity sharing across the enterprise.
F6	The Enterprise Identity Management Framework shall provide the capability for single sign-on across partner web applications.
F7	The Enterprise Identity Management Framework shall provide the capability for single sign-on to participating state, tribe, or local government web applications using an identity issued by an EPA system.
F8	The Enterprise Identity Management Framework shall provide the capability for single sign-on to participating EPA web applications using an identity issued by a state, tribe, or local government system.
F9	The Enterprise Identity Management Framework shall provide the capability for single sign-on to participating state, tribe, or local government web applications using an identity issued by another participating state, tribe, or local government system.
F10	The Enterprise Identity Management Framework shall provide the capability to access partner web services using shared credentials.
F11	The Enterprise Identity Management Framework shall provide the capability to access participating state, tribe, or local government web services using an identity issued by an EPA system.
F12	The Enterprise Identity Management Framework shall provide the capability to access participating EPA web services using an identity issued by a state, tribe, or local government system.
F13	The Enterprise Identity Management Framework shall provide the capability to access participating state, tribe, or local government web services using an identity issued by another participating state, tribe, or local government system.
F14	The Enterprise Identity Management Framework shall provide a mechanism to establish authorization policies that can be enforced by partner applications.
F15	The Enterprise Identity Management Framework shall provide a shareable component that can be responsible for all the handshaking with identity providers (IDPs) on behalf of the relying party (RPs).
F16	The Enterprise Identity Management Framework shall establish a common set of user attributes to be used across the enterprise.
F17	The Enterprise Identity Management Framework shall establish a governance framework that defines the policies that regulate and control the exchange of identity information between partners.
F18	The Enterprise Identity Management Framework shall be flexible enough to allow for partners to directly accept identities from approved partner organizations assuming Enterprise Identity Management standards and governance policies are used.
F19	The Enterprise Identity Management Framework and associated governance shall seek to minimize impacts on related services such as Shared CROMERR Services (SCS) and to be fully compatible with SCS.

F20	The Enterprise Identity Management Framework shall be flexible enough to allow for partners to participate to the extent that makes the most sense for their organization.
F21	Participation in the Enterprise Identity Management Framework shall be voluntary.
F22	Participating organizations shall accept external users authenticated by third parties.
F23	Participating organizations shall issue credentials capable of being utilized by other participating organizations.
F24	The Enterprise Identity Management Framework shall include a governance process by which the common set of user attributes to be supported can be maintained (attributes added, modified, and deprecated).
F25	The Enterprise Identity Management Framework shall establish a governance framework that defines policies and procedures to implement a Help Desk for users and participating partners.
F26	Participating organizations shall be allowed to terminate their participating in the Enterprise Identity Management Framework at any time.
F27	The Enterprise Identity Framework shall support the identities of multiple types of users including co-regulators, regulated entity, and public.
F28	The Enterprise Identity Management Framework shall provide support capabilities (e.g. documentation, audit processes, etc.) and services that align to EPA's Shared CROMERR Services initiative to streamline the ability of partners to implement CROMERR compliant applications.
F29	The Enterprise Identity Management Framework shall provide the capability to update user attributes associated an identity and have those changes shared with partners through identity mapping (transformation) services.
F30	All components of the ultimate solution for implementing the Enterprise Identity Management Framework shall be fully documented to include information on system design and specifications, system operations, and implementation instructions. This documentation will be sufficiently detailed and readily available so that potential relying parties and identity providers can understand, evaluate, and implement the solution.
F31	All components of the ultimate solution for implementing the Enterprise Identity Management Framework shall be operated and supported in a manner that is consistent with other critical information technology services. The solution will include a product roadmap, a standard and transparent patch and release schedule, provisions for backup and redundancy, and a robust staffing plan for operational support.
F32	All components of the ultimate solution for implementing the Enterprise Identity Management Framework shall meet collaboratively established performance standards to ensure adequate system capacity and minimize the risk of service interruption.

4.3 Key Technical Requirements

The work group collaboratively identified the key technical requirements for the EIDMS that are described in this section. This list is not comprehensive but seeks to identify the key, high-level requirements that must be supported by the system.

Exhibit 4-3 Technical Requirements

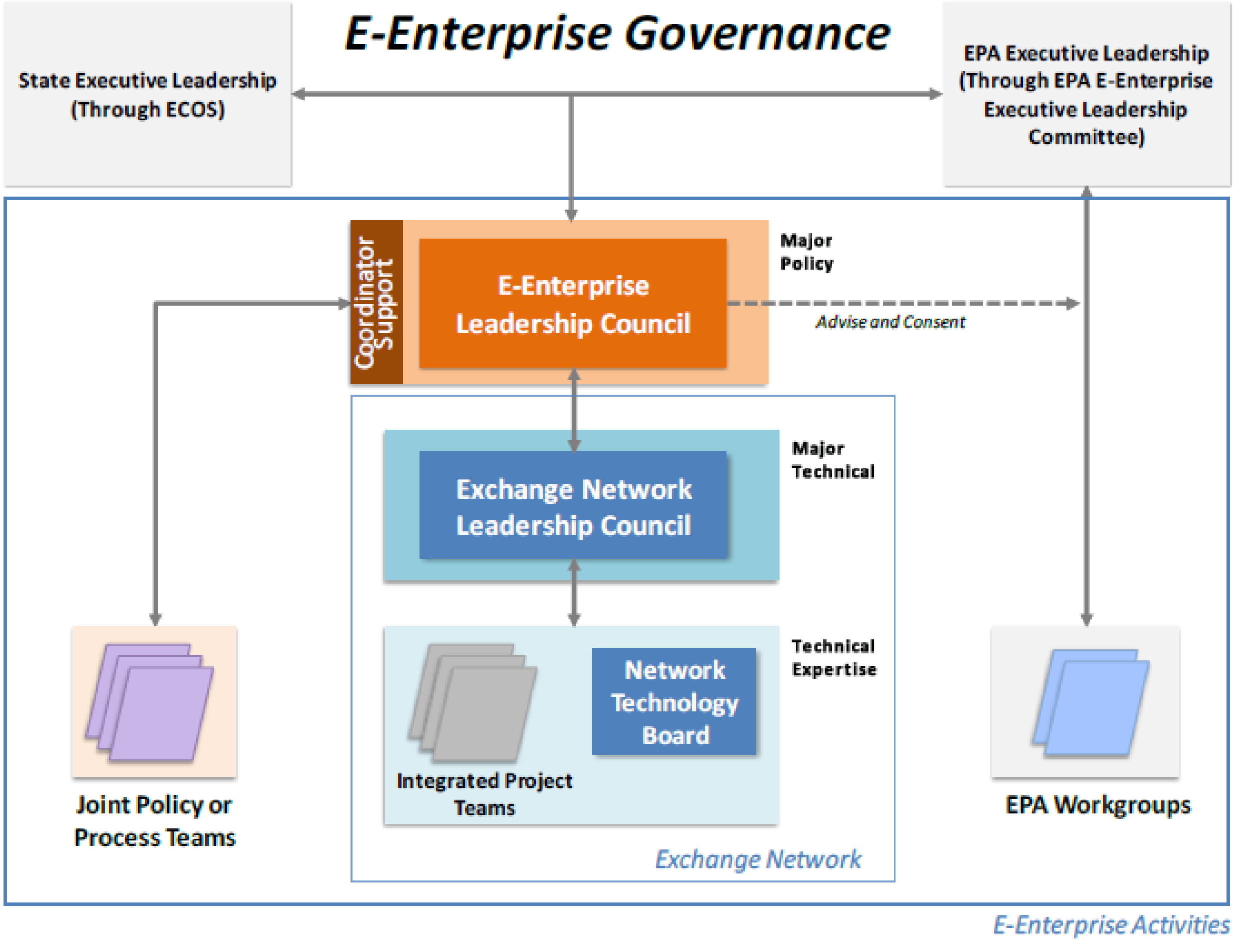
Number	Description
T1	The Enterprise Identity Management Framework shall be built upon open, technical specifications and identity federation standards to minimize integration efforts and maximize interoperability.
T2	The Enterprise Identity Management Framework shall be able to consume multiple identity providers and provide protocol negotiation to relying parties.
T3	The Enterprise Identity Management Framework shall provide identity mapping (transformation) services from identity providers to relying parties.
T4	The Enterprise Identity Management Framework identity mapping service will support a defined UserID attribute.
T5	The Enterprise Identity Management Framework identity mapping service will support a defined Status attribute.
T6	Identity providers within the Enterprise Identity Management Framework shall maintain a password or alternative security/credential device for every identity.
T7	The Enterprise Identity Management Framework identity mapping service will support a defined Email attribute.
T8	The Enterprise Identity Management Framework identity mapping service will support a defined Address attribute.
T9	The Enterprise Identity Management Framework identity mapping service will support a defined Address2 optional attribute.
T10	The Enterprise Identity Management Framework identity mapping service will support a defined City attribute.
T11	The Enterprise Identity Management Framework identity mapping service will support a defined State attribute.
T12	The Enterprise Identity Management Framework identity mapping service will support a defined ZipCode attribute.
T13	The Enterprise Identity Management Framework identity mapping service will support a defined Phone attribute.
T14	The Enterprise Identity Management Framework identity mapping service will support a defined Title attribute.
T15	The Enterprise Identity Management Framework identity mapping service will support a defined FirstName attribute.
T16	The Enterprise Identity Management Framework identity mapping service will support a defined MiddleInitial attribute.
T17	The Enterprise Identity Management Framework identity mapping service will support a defined LastName attribute.
T18	The Enterprise Identity Management Framework identity mapping service will support a defined NameSuffix attribute.
T19	The Enterprise Identity Management Framework identity mapping service will support a defined Organization attribute.
T20	The Enterprise Identity Management Framework identity mapping service will support a defined attribute that indicates the standard Level of Assurance (LOA) level for the identity being provided.
T21	The Enterprise Identity Management Framework identity mapping service will support an attribute that can indicate a custom Level of Assurance (LOA) level (as needed for something like CROMERR, for example) for the identity being provided.
T22	The Enterprise Identity Management Framework identity mapping service will support defined attributes that support an identity to be associated with a foreign address.
T23	All network traffic within the Enterprise Identity Management Framework will be secured/encrypted.
T24	Centralized or shared portions of the Enterprise Identity Management Framework shall be architected and deployed to maintain 99.9% uptime.

T25	The Enterprise Identity Management Framework participant organizations shall have auditable security processes.
T26	The Enterprise Identity Management Framework shall include services that allow for the reporting of account tampering/compromise.
T27	The Enterprise Identity Management Framework shall include sufficient logging and debugging services to allow relying party system developers self service capabilities investigating authentication events.
T28	The Enterprise Identity Management Framework participant organizations shall utilize the framework services to alert other participant organizations of incidents of account tampering or other security threats.
T29	The Enterprise Identity Management Framework will have multiple environments including: development, testing, and production.

4.4 Enterprise Identity Governance

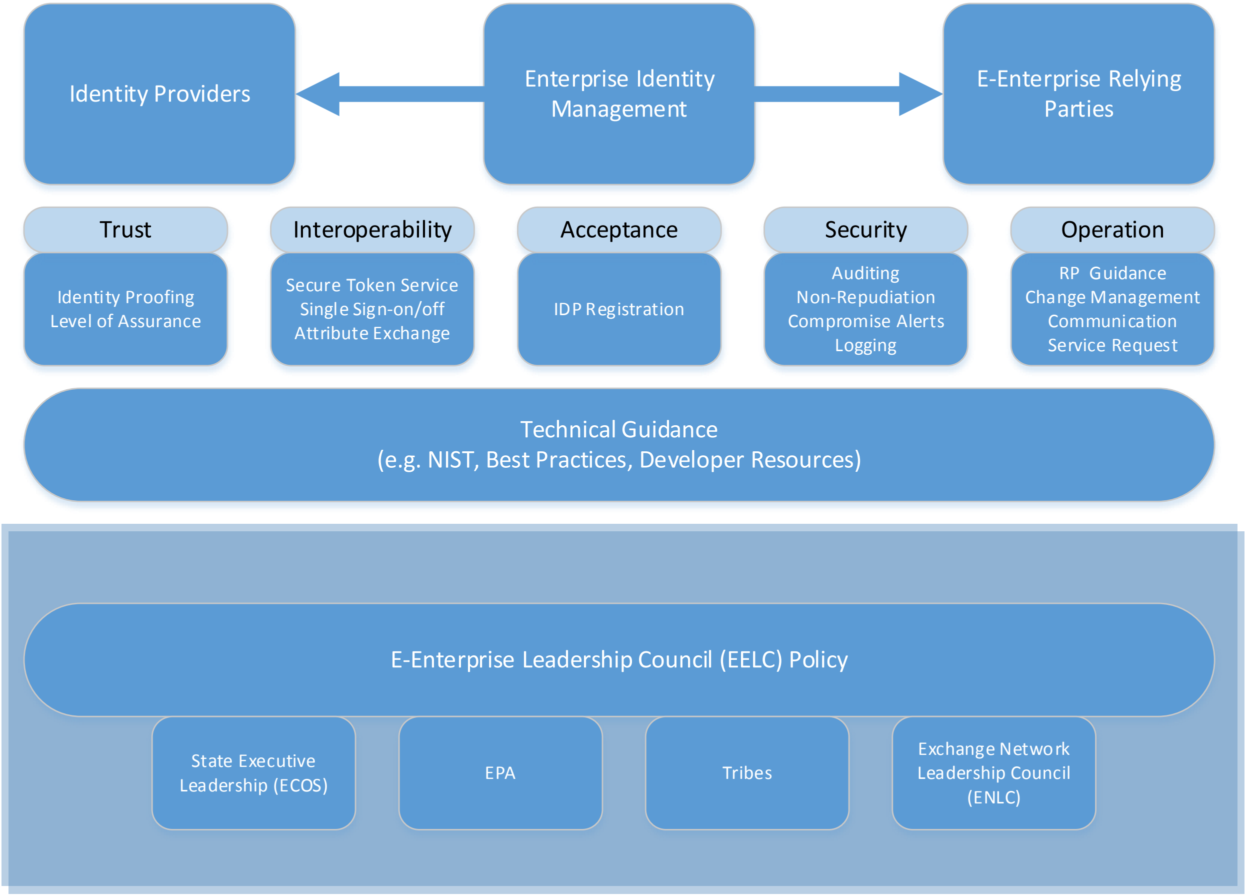
The importance of partnership within E-Enterprise was identified explicitly by the State-EPA E-Enterprise Working Group's Blueprint Team as Design and Operating Principle #1 (Partnership of Environmental Government Regulators). Complex partnerships such as the Exchange Network and E-Enterprise require a governance structure to guide the partnership and to establish rules, policies, and procedures related to the various aspects of operation. The E-Enterprise Leadership Council (EELC) is the state and EPA joint governance body for E-Enterprise. The EELC is patterned after the successful governance body of the Exchange Network, the Exchange Network Leadership Council (ENLC). Similar to how the ENLC provides coordination and oversight for the Exchange Network, the EELC will provide coordination and oversight for E-Enterprise. The governance structure seeks to provide leadership, establish trust among partners, set clear expectations, and provide transparency and flexibility. The ENLC will be integrated with the E-Enterprise governance structure providing technical expertise as depicted in Exhibit 4-4. For more information on overall E-Enterprise joint governance, see Section 6: State and EPA Joint Governance of E-Enterprise in the Blueprint.

Exhibit 4-4 E-Enterprise Joint Governance Structure


E-Enterprise Governance
State Executive Leadership (Through ECOS)
EPA Executive Leadership (Through EPA E-Enterprise Executive Leadership Committee)
Coordinator Support
E-Enterprise Leadership Council
Major Policy
Advise and Consent
Exchange Network Leadership Council
Major Technical
Network Technology Board
Integrated Project Teams
Technical Expertise
Joint Policy or Process Teams
EPA Workgroups
Exchange Network
E-Enterprise Activities

Enterprise identity management will require governance around a specific set of rules, policies, and technical decisions. As a subset of E-Enterprise governance responsibility, EIdM governance will fall under the umbrella of the EELC. This will bring together the partnerships established through the EELC including state executive leadership through ECOS as well as the technical expertise and structure provided by the ENLC and its Network Technology Board (NTB). Ultimately the EELC will provide technical and procedural guidance related to several categories that will impact how various components will be brought into and operate within the EIdM (Exhibit 4-5). The EELC structure is already modeled upon the successful structure of the Exchange Network and the overall E-Enterprise joint governance model incorporates the ENLC as well as the Exchange Network's Network Technology Board. As this EIdM effort moves forward, these models should be explored further as examples. In addition, other efforts focused on identity federation, such as GSA's [id]MANAMGENT.GOV PMO, have laid some groundwork that may be able to be leveraged as EIdM moves forward.

Exhibit 4-5 E-Enterprise Identity Management Governance Framework



Various rules and procedures related to EIdM will fall into one or more of the following categories of governance:

- Trust – Rules and guidelines, primarily related to identity providers, around identity proofing and level of assurance.
- Interoperability – Primarily technology guidance and decisions around protocol and tool selection that will help EIdM provide a seamless user experience to users.
- Acceptance – Registration and adoption processes for becoming an E-Enterprise identity provider.
- Security – Rules and guidance related to mitigating security risks to E-Enterprise and its partner organizations.
- Operation – Guidance to partners seeking to be service providers, or relying parties, within EIdM, change management functions, communication, and service requests.

4.4.1 Enterprise Identity Management Governance Processes

Detailing the critical partner administrative procedural requirements needed to support the EIdM is identified in the Charter for the E-Enterprise Shared Identity Management System Scoping Work Group as subsequent phase of work. The contents of this Concept of Operations will be used to inform the scope of subsequent phases. During work group efforts several important areas or topics related to governance were identified and are documented in this section and are to be more fully defined and expanded upon in subsequent phases of EIdM planning. These governance areas may be expanded upon in subsequent efforts to include more detailed process information, roles and responsibilities, workflow, metrics, and supporting tools and technologies.

4.4.1.1 Service Strategy

EIdM governance will establish the overall identity management service strategy. The service strategy includes processes associated with:

- Portfolio Management – Processes associated with determining which partner organizations and services will participate in EIdM
- Financial Management – Processes possibly associated with providing integration support through grants, and support for operations and service desk
- Relationship Management – Establishing and maintaining relationships with states, tribes, local government, and EPA program offices
- Functional and Business Architecture Management – Establishing and maintaining the EIdM functional and business architecture

4.4.1.2 Continual Service Improvement

EIdM governance will be responsible for continually reviewing and improving upon the EIdM service.

Processes include:

- Ongoing assessment of potential services to integrate with EIdM
- Establishment of key performance indicators

- Tracking and review of key performance indicators
- Recurring or ongoing stakeholder (user, RP, and IDP) communication

4.4.1.3 Service Transition

EIdM governance will be responsible for managing the transition from planning and design into development and implementation.

Processes include:

- Establishing partner onboarding processes (See Sections 4.4.1.6 and 4.4.1.9)
- Establishing partner offboarding processes
- Management of the development lifecycle
- Release management
- Configuration management
- Change management

4.4.1.4 Program Management and Operations

Program management falls into two main categories. These are related to high-level decision making (budget, communications, roles and responsibilities, etc.) and around lower level, day-to-day operations of the EIdM. This work group's parent IPT, the E-Enterprise Architecture Integrated Project Team, is working through similar process and governance decisions related to the E-Enterprise Portal governance model. Program management will likely primarily be the responsibility of some combination of OEI and OCFO. Subsequent governance decisions for project management and operations related to EIdM should follow the direction taken related to governance of the E-Enterprise Portal.

4.4.1.5 Identity Provider Registration/Adoption

Establishing trust between partners is a foundational key to success in EIdM. Strong governance in general is key to establishing trust. Particularly important related to the establishment of trust within the governance processes are those related to the onboarding of partners. The identity provider services must be able to dependably meet the assurance needs of relying parties who will trust the identities provided by identity providers. The processes by which identity providers will be approved and integrated into EIdM are key to establishing and maintaining trust among the partner organizations.

Processes include:

- Establishment of identity provider application
- Processing and review of identity provider application, including:
  - Service Level Agreements (SLAs) that govern IDP performance requirements
  - Security assessment (possibly performed by an independent assessor)
- Determination of identity provider assurance level

- Approval/Denial of identity provider application

Two related areas of governance (4.4.1.7 and 4.4.1.8) are noted individually in this list of key governance topics.

4.4.1.6 Determination of Identity Provider Assurance Level

Closely related to its parent governance area, Identity Provider Registration/Adoption, this area of governance includes all processes that support the determination of level of assurance that an identity provider is able to support.

Processes include:

- Adoption of standard level of assurance definitions for EIdM
- Review of identity provider registration information
- Assignment of EIdM level of assurance to perspective identity provider

4.4.1.7 Identity Provider Policy Conformance Auditing

This governance area includes processes for ensuring that identity providers that are participating in the EIdM service maintain the necessary requirements to continue participation in EIdM and to verify that their assigned level of assurance remains appropriate. Identity provider policies, processes, and controls may change over time. This area of governance exists to maintain trust within the enterprise by continually confirming that identity providers conform to all EIdM requirements.

Processes include:

- Auditing identity providers after registration to ensure that they continue to comply/conform with all required policies and security requirements
- Identity provider reporting processes that allow identity providers to report changes that might impact their level of assurance and/or eligibility to participate in the enterprise

4.4.1.8 Relying Party Registration/Adoption

Similar to the Identity Provider Registration/Adoption area of governance, Relying Party Registration/Adoption governance is fundamental to establishing and ensuring a framework of trust between partners. The processes by which relying parties will be approved and integrated into EIdM are key to establishing and maintaining trust among the partner organizations.

Processes include:

- Establishment of relying party application
- Processing and review of relying party application
- Determination of assurance level requirement
- Approval/Denial of relying party application
- Relying party implementation guidance

Two related areas of governance (4.4.1.10 and 4.4.1.11) are noted individually in this list of key governance topics.

4.4.1.9 Determination of Identity Assurance Level Requirement

Closely related to its parent governance area, Relying Party Registration/Adoption, this area of governance includes all processes that support the determination of the assurance level requirement for services that relying parties seek to provide through EIdM.

Processes include:

- Adoption of standard level of assurance definitions for EIdM
- Review of relying party registration information
- Providing Assignment of recommended EIdM level of assurance to for relying party services

4.4.1.10 Relying Party Identity Assurance Level Conformance Auditing

This governance area includes processes for ensuring that relying parties that are participating in the EIdM service maintain the necessary requirements to continue participation in EIdM and to verify that their assigned level of assurance requirements remain appropriate. Relying party policies, processes, and controls may change over time. This area of governance exists to maintain trust within the enterprise by continually confirming that relying parties conform to all EIdM requirements.

Processes include:

- Auditing relying parties after registration to ensure that they continue to comply/conform with all required policies
- Relying party reporting process that allow relying parties to report changes that might impact their level of assurance requirements and/or eligibility to participate in the enterprise

4.4.1.11 Attribute and Protocol Guidance and Adoption

This area of governance relates to the attribute exchange services supported through EIdM (Section 4.5.1.3.2). Over time the standard set of attributes supplied through the EIdM service and its identity providers may be required to change. Reasons for modifying the attribute definition could include meeting government standards, minimizing any possible technical risk, maximizing interoperability, or responding to privacy concerns.

Processes include:

- Addition of attributes to the attribute profile
- Modification of existing attributes in the attribute profile
- Removal of attributes from the attribute profile
- Management of technical standards and protocols associated with the exchange of attribute profile

4.4.1.12 Maintain Developer Resources

This is a technical area of governance that aims to serve as a resource to partner developers who are integrating with EIdM. It is likely that EIdM related developer resources will be provided as a subset of resources made available and governed by processes established at the E-Enterprise level. Developer resources may include tools such as Software Development Kits (SDK) application program interfaces (APIs), sample code, a knowledgebase, etc.

4.4.1.13 Establish guidelines for security

Security is a concern for all organizations that will participate in EIdM. This governance area seeks to establish and maintain trust by putting policies, procedures, and controls in place across the enterprise that mitigate security risks.

Processes include:

- Establishment of security related guidelines related to encryption of data in transit and at rest and for the handling of personally identifiable data (PII) for partner domains and applications
- Establishment of auditing requirements for any centralized EIdM components as well as partner systems
- Establishment of logging requirements for any centralized EIdM components as well as partner systems
- Establishment of processes and mechanisms for communicating security alerts within the enterprise

4.4.1.14 Incident Management/Help Desk

This governance area will be closely associated to E-Enterprise level governance related to the establishment of a help/service desk to respond to issues raised with the operation of E-Enterprise. EIdM specific issues will occur and the establishment of a communication approach and issue resolution workflow will be required.

Processes include:

- Integration with E-Enterprise level incident management
- Establishment of help desk process and communication approach related to EIdM specific E-Enterprise issues

4.5 Description of Solution Functionality

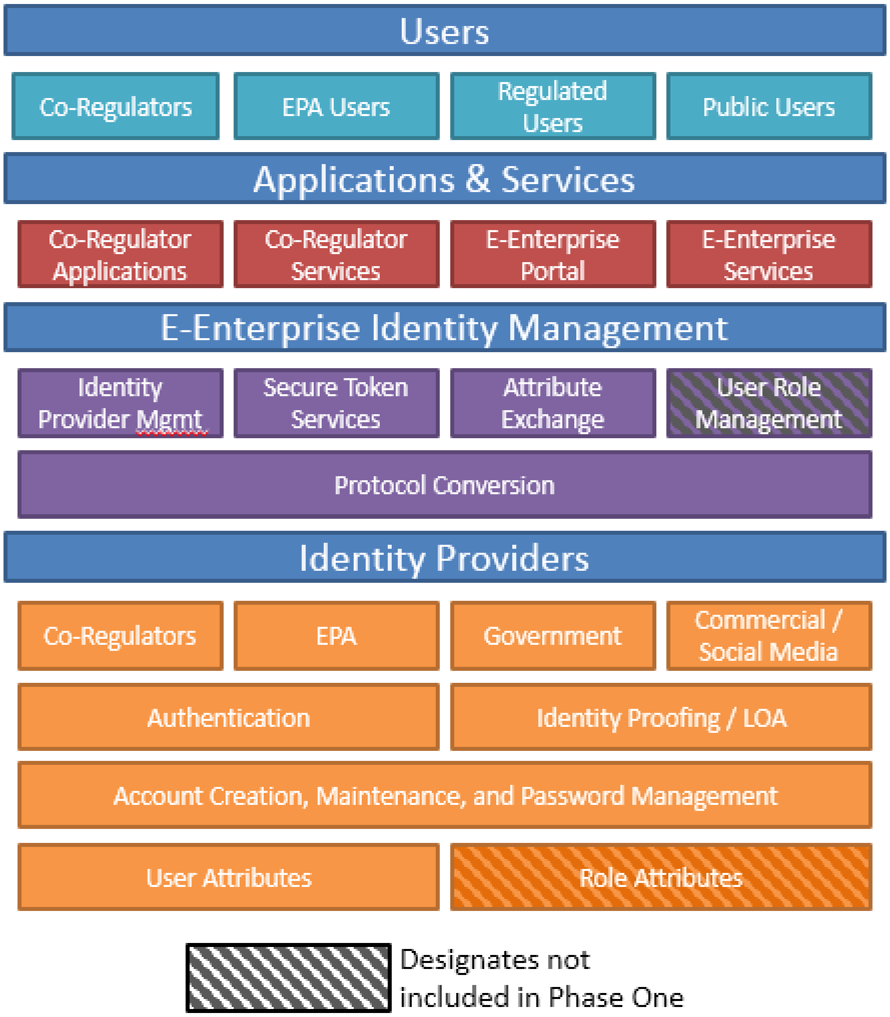
The E-Enterprise Shared Identity Management System will extend identity management above the single-domain level and create a security trust between participating organizations (multiple domains). Participating organization's systems will share identity attributes based on agreed upon standards. In addition, the system will facilitate the authentication of identities by other participating organizations. This system will include multiple identity providers where each provider includes services related to user registration and authentication for a subset of E-Enterprise related users with identities shared across the enterprise.

In addition to the system itself, there will be a governance model (Section 4.4) that establishes the trust relationships between participating organizations.

4.5.1 Functional Architecture

After discussing federal identity management initiatives such as Connect.Gov as well as work group member experiences, the work group came to the consensus that as a key infrastructure component of E-Enterprise, identity management will function as a bridge, or hub, between users and the systems or services that they attempt to access, and the identity providers responsible for registering, sharing attributes, and authenticating the users.

Exhibit 4-6 High-Level Functional Architecture



4.5.1.1 Users

The E-Enterprise Portal and E-Enterprise partner systems will support multiple types of users, including:

- Co-Regulators – Users who are also members or staff of partner environmental government regulators. Co-regulators could be state, tribe, or local government environmental regulators.
- EPA Users – Users who are also members or staff of the EPA.
- Regulated Users – A user who is acting on behalf of themselves or a company or facility that is subject to federal, state, tribal, or local environmental regulation.
- Public Users – A user who is a member of the public and is not acting on behalf of a regulatory agency or regulated entity.

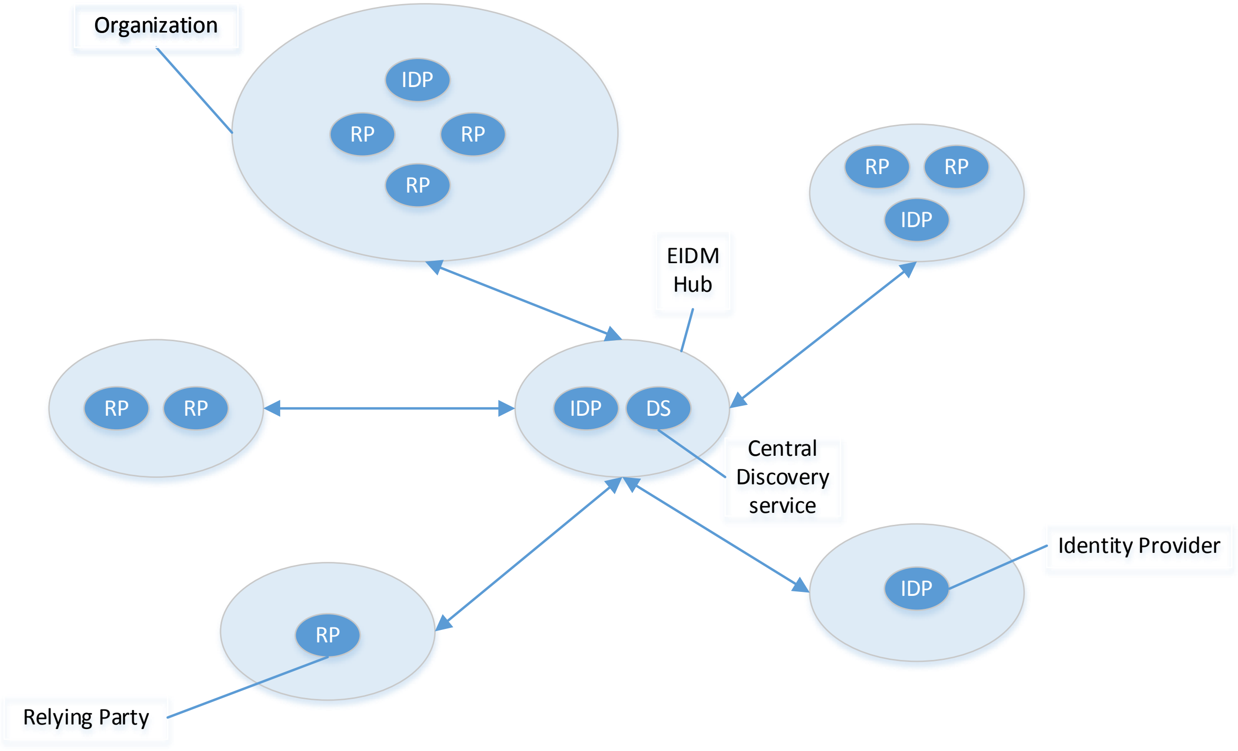
4.5.1.2 Applications and Services

Users will be able to interact with E-Enterprise through multiple applications and services. In some cases these interactions will be through E-Enterprise specific resources such as the E-Enterprise Portal or other E-Enterprise services. These user interactions could also be initiated through co-regulator portals, applications, or services. E-Enterprise interoperability principles and goals come into play when a user seeks to navigate, either through a user interface or through a behind the scenes service, between E-Enterprise related resources.

4.5.1.3 E-Enterprise Identity Management

Enterprise identity management serves as a bridge, or hub, between E-Enterprise resources and multiple identity providers. Implementing enterprise identity management as a central service of the E-Enterprise infrastructure will provide a flexible and scalable solution for supporting the trust relationships between partners in the enterprise. Each partner, or organization, plays at least one of two roles within the enterprise. An organization can function as an identity provider for the enterprise. In addition, an organization can contain one or more applications (relying parties) that rely on identities provided by the identity providers.

Exhibit 4-7 E-Enterprise Identity Management Network



In order to support the network of relying parties and identity providers, the E-Enterprise Identity Management layer must provide a comprehensive set of identity federation functionality.

4.5.1.3.1 Protocol Conversion

A federation service, or hub, can support the differences in standards and protocols used by different identity providers by performing protocol conversion as needed. As standards are adopted by the E-Enterprise governance bodies, support for the standards can be provided once within the enterprise identity management hub as opposed to each service provider, or relying party, in the enterprise developing support for the newly adopted standards or protocols. A federation service can also decrease maintenance cost for participating organizations as open standards are updated or deprecated.

4.5.1.3.2 Attribute Exchange

In addition to differences in protocol, an identity hub can facilitate standardization of user attribute, or identity, information across the enterprise. Different identity providers in an enterprise as diverse as E-Enterprise will have differences in their provisioning processes and in the collection of identity attributes. An identity hub can function as a centralized attribute exchange point for consuming attribute data in different forms from identity providers and supplying relying parties with a single, agreed upon set and format of attributes. This provides the enterprise with the same flexibility and scalability benefits as central protocol conversion. As changes are made in attribute definition for E-Enterprise by governance bodies, the identity hub will provide a point to focus the majority of required implementation changes, as opposed to forcing significant burden on multiple partners.

4.5.1.3.3 Identity Provider Management

An identity hub provides a central service for the management of identity providers. Centralization of these tasks:

- Reduces burden to relying parties within the enterprise by removing the need for the relying party to implement integration with multiple identity providers.
- Improves the user’s experience by providing the same login process through each service supported by the enterprise.
- Promotes identity sharing by making it more likely for a user to utilize the same identity across the enterprise.
- Increases security by creating a single location for updating the level of assurance associated with an identity provider and by supporting the quick and universal removal of an identity provider from the enterprise.

4.5.1.3.4 Secure Token Services

Some protocols rely heavily on web browser features and are therefore limited to use in web applications. E-Enterprise Component #5, E-Enterprise Open Data and Web services, describes a network of web services to be made available to E-Enterprise applications. While many such web services will be publically available, some will be required to be secure. The use of tokens generated by a service in an identity hub can support providing a seamless user experience and single sign-on as users move between related applications as well as when accessing secure web services.

4.5.1.4 Identity Providers

Communication with identity providers will be managed through a centralized identity hub. The E-Enterprise Identity Management System will federate identities provided by multiple identity providers. The available identity providers are likely to include:

- Co-Regulator Identity Providers
- EPA Identity Providers
- Other Government Identity Providers
- Commercial/Social Media Identity Providers

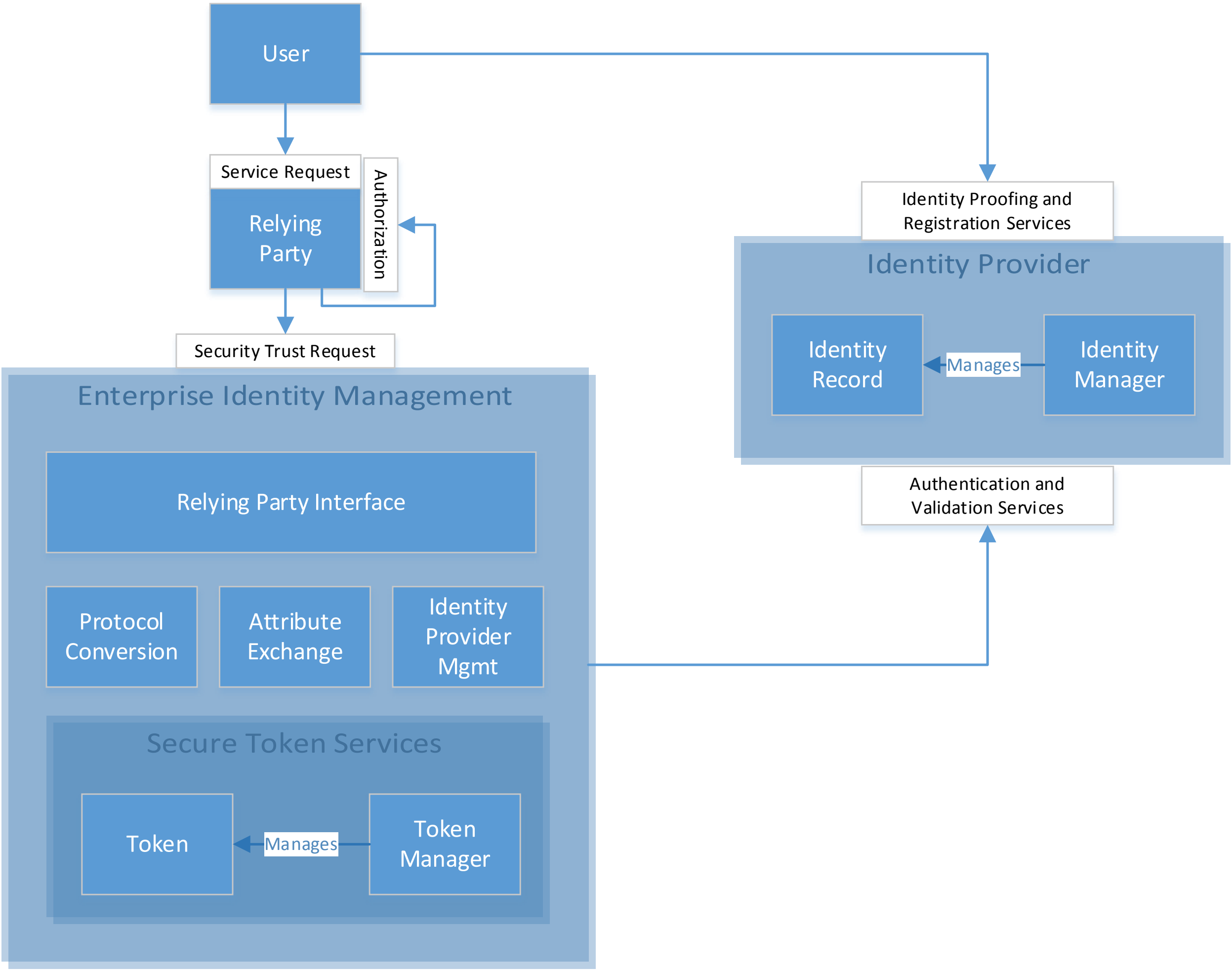
Users will directly interact with one or more identity provider through the act of registration. Identity providers will be responsible for:

- The identity proofing of registered users
- Maintaining the requirements for the level of assurance to which they are assigned through the identity hub's identity provider management (Section 4.5.1.3.3) functionality.
- Registration/provisioning activities such as account creation, maintenance, user attribute storage, and password management.
- The authentication of users requesting to login through the identity hub.

4.5.2 E-Enterprise Identity Management Interaction

The interaction between the major entities, or layers, in the High Level Functional Architecture diagram (Exhibit 4-6), describes the core process steps that will support identity federation. Those interactions are depicted in Exhibit 4-8.

Exhibit 4-8 Relying Party and Identity Provider Interaction



A user initiates interaction with the framework primarily through one of two interactions. Generally speaking, the first action that a user participates in that is directly related to enterprise identity management is through registration services at an E-Enterprise identity provider. The user must have a digital identity that they will assume when interacting with E-Enterprise applications and services. Depending on the types of actions the user desires to engage in within E-Enterprise, they may choose to register with an identity provider that maintains a level of assurance high enough to require some form of identity proofing to be performed at the time of registration.

When the user interacts with an application or service (a relying party) that is secured or otherwise requires them to be authenticated, they will be redirected to the EIDMS's Relying Party Interface. This interface will provide the user with the list of E-Enterprise identity providers that have been approved through the necessary governance processes. When the user selects their preferred identity provider they will be redirected again to the identity provider who will authenticate the user and validate to the level of assurance that they can provide that the user is who they say that they are.

The EIDMS identity hub will perform any necessary protocol conversions based on the standards and protocols employed by the identity provider. The hub will also perform steps to transform the identity attribute data provided by the identity provider into the standard format agreed upon for exchange through E-Enterprise. The user will be redirected back to the relying part with their positive assertion as well as a token generated by the Secure Token Services that can be used to provide proof of authentication to any subsequent actions within E-Enterprise.

Finally, each relying party is responsible for user authorization. The identity hub will help facilitate the authentication of the user by the identity provider and returning the assertion of that authentication to the relying party. Partner organizations and their rely party applications remain autonomous in how they authorize users to perform actions.

4.6 Constraints

Enterprise identity management can provide many benefits, some of which have been discussed in previous sections of this document (Section 3.2). While there are many benefits, enterprise identity management also has implications and possible constraints within the context of E-Enterprise:

- Standards – There are many standards in usage within government and industry to support identity federation. Selecting which standards to support is a challenge. Employing an identity hub model does reduce the impact to individual applications when accepted standards proliferate, but choosing standards and implementing them within the attribute exchange and protocol conversion services of enterprise identity management does represent a challenge and possible increased complexity in the solution.
- Security – There are trade-offs related to security in enterprise identity management. The solution provides a mechanism for easier control of user provisioning. Through governance the framework can decide what information about a user is passed between partner organizations. Examples of information that can serve to increase security are information about when users may have left a participating organization, or the sharing of notifications when there is suspicious account activity or evidence that an account has been compromised. Providing functionality like single sign-on through secure tokens does represent a risk, however, in that freer rein may be given to users who would succeed in compromising the system.
- Relationships and Trust – The foundation of a successful enterprise identity management solution or framework is building relationships and trust. There are technical complexities, but for an implementation to be successful partner organizations within the enterprise must be able to trust one another to follow the agreed upon governance rules and guidelines and to implement the appropriate security controls and measures to keep the enterprise safe and secure.
- Effort – While an identity hub model does reduce the cost of effort associated with adoption of identity federation, effort is still required to be a partner in the enterprise. Relying party applications must be integrated with the identity hub, which will then manage the integration with multiple identity providers. In the case of new systems that will participate, identity federation likely represents a savings in effort in that user registration and authentication pieces can be omitted from system design and development. The cost benefit in terms of effort between retrofitting a system to participate and ongoing time and maintenance related to user provisioning and authentication is more difficult to calculate. There will be required effort of any participating organization and this may be a constraint in terms of adoption.
- Adoption – The noticeable benefits to the user experience are dependent on partner participation. The more partner organizations participate, the more relying party applications and services function seamlessly, the better the user experience will be. It is also possible that the more secure services participate, that there will be fewer barriers to providing quality aggregated environmental data not only to the public, but also to environmental regulators, emergency responders, and decision makers. Potential participating organizations may see some of these risks and constraints as well as other internal constraints as barriers to adoption that will weaken the benefits of the potential enterprise as a whole.

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

4.8 Evaluation Criteria

Evaluation and selection of EIdM service components will be the responsibility of E-Enterprise and EIdM governance (Section 4.4.1.3). Input from the E-Enterprise Shared Identity Management System Scoping Work Group in the form of the contents of this Concept of Operations document will inform the establishment of final evaluation criteria and eventual short and long term service selection for EIdM.

The following criteria will be considered for inclusion in the EIdM governance evaluation criteria for the EIdM service selection:

- Provides a lower barrier to adoption and participation for E-Enterprise partners
- Employment of widely used standards, protocols and specifications (non-proprietary approach)
- Provides required support to establish a framework of security trusts
- Minimization of integration burden on relying parties and identity providers
- Promotes identity sharing and registration re-use
- Provides single sign-on across partners and systems
- Minimization of costs per transaction
- Meets business, functional, and technical requirements expressed in Concept of Operations
- Builds confidence, trust, and assurance among relying parties and identity providers through transparent and collaborative system design and operation

Appendix A. Glossary and Terms

The following is a list of terms used in this document.

Term	Definition
Approved Identity Provider (AIP)	An identity provider (see Identity Provider) approved as a partner in the EIDMS.
Assurance	1) The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
Assurance Level	See Level of Assurance.
Authentication	The act or process of determining that a person or user is who they claim to be.
Authorization	The act or process of determining which permissions or roles that a user has within a system.
E-Authentication	The process of establishing confidence in user identities electronically presented to an information system. See National Institute of Standards and Technology Electronic Authentication Guideline.
E-Enterprise	E-Enterprise for the Environment (E-Enterprise) is a U.S. EPA-state initiative to improve environmental performance and enhance services to the regulated community, environmental agencies, and the public. See E-Enterprise for the Environment Conceptual Blueprint: Principles and Components.
Enterprise Identity Management (EIdM)	An approach for managing identities and access to systems and services that cross security domains.
Enterprise Identity Management System (EIDMS)	The technical solution and its components that will support the concept for proposed solution for E-Enterprise Shared Identity Management.
Federated Identity Management (FIdM)	See Enterprise Identity Management.
Federation	See Enterprise Identity Management.
Identity Management (IdM)	The combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguarding of personal identity information. The primary goal of the Identity Management process is to assign attributes to a digital identity and to connect that identity to an individual. See National Science and Technology Council Identity Management Task Force Report.
Identity Provider (IDP) (IdP)	An entity responsible for providing user identifiers for users looking to access a system and asserting to other systems that the user is known to the provider.
Identity Store	Any system, whether participating in federation or not, that stores a user's identity information.

Level of Assurance (LOA)	Also referred to as Assurance Level. The measure of assurance, or degree of confidence, in an authentication service or mechanism. There are four standard levels of assurance: • Level 1: Little or no confidence in the asserted identity's validity. • Level 2: Some confidence in the asserted identity's validity. • Level 3: High confidence in the asserted identity's validity. • Level 4: Very high confidence in the asserted identity's validity. See E-Authentication Guidance for Federal Agencies Memorandum (M-04-04).
Relying Party (RP)	A server providing access to secure software relying on an identity provider for user authentication and information.
Secure Token Service (STS)	A service responsible for issuing security tokens that create a chain of trust and can be used to facilitate single sign-on.
Service Provider (SP)	See Relying Party.