Joining the U.S. E-Authentication Identity Federation

Business Owner: Federation Management
Creation Date: 5/30/2007
Last Updated: 9/26/2007
Version: EA-MG-0077-1.0-F
Audience: Public

Document History

Status	Release	Date	Comment	Audience
Template	0.0.0	5/30/07	Outline	Internal
Template	0.0.1	6/4/07	Outline	PMO
Template	0.0.2	6/6/07	Revised per Myisha Frazier-Mcelveen comments	Internal
Draft	0.0.3	6/13/07	Michael Heel – wrote Phase I section of document	Internal
Draft	0.0.4	6/14/07	Michael Heel updated Phase I to reflect comments of team	Internal
Draft	0.0.5	6/14/07	Phase II added to document	Internal
Draft	0.0.6	6/15/07	Ali’s Comments on Phase I & Phase II partially written	Internal
Draft	0.0.7	6/20/07	Boarding Phase written	Internal
Draft	0.0.8	6/22/07	Acceptance Testing & Rollout phases added	Internal
Draft	0.0.9	6/25/07	Dave’s & Andrew’s Comments incorporated	Internal
Draft	0.0.10	6/28/07	Ali reviewed and edited document	Internal
Draft	0.0.11	6/28/07	Mike reviewed and edited document	Internal
Draft	0.0.12	7/1/07	Continued revision	Internal
Draft	0.0.13	7/2/07	Document prepared for internal review	Internal
Draft	0.0.14	7/9/07	Revised per internal red team review	Internal
Draft	0.0.15	7/9/07	Revised per internal review	Internal
Draft	0.0.16	7/10/07	Revised per internal review	Internal
Draft	0.1.0	7/11/07	Revised per internal review	PMO
Draft	0.1.1	8/14/07	Application of PMO’s comments	Internal
Draft	0.1.2	8/20/07	Application of Treb’s Comments	Internal
Draft	0.1.3	8/22/07	Planning & Analysis updated to reflect new CS Project Plan	Internal
Draft	0.2.0	8/22/07	Revised per internal review	PMO
Draft	0.2.1	9/12/07	Revised per PMO comments	Internal
Draft	0.2.2	9/20/07	Revised per Internal comments	PMO
Draft	0.2.3	9/24/07	Revised per Internal comments	PMO
Draft	1.0.0	9/26/07	Final	PMO

Editors

Dave Silver	Alexis Wells	Michael Heel
Andrew Chiu	Treb Farrales	

Executive Summary

Joining the U.S. E-Authentication Identity Federation (Federation) requires successful completion of various activities in a particular order. The activities include, but are not limited to executing agreements, understanding requirements, implementing technology and support services, assessing compliance, and making E-Authentication-enabled services accessible to end users. This document highlights the flow and relationship of those activities in order to provide a useful, usable “roadmap” for joining the Federation. In doing so, the roadmap optimizes and expedites the process, while reducing risk and uncertainty.

The roadmap uses a phased approach: Planning and Analysis, Design and Development, Boarding, Acceptance Testing, and Rollout. Description of each phase is in terms of essential tasks, general flow, inputs, outputs, and milestones. This roadmap is a tool that supports and facilitates a System Owner’s E-Authentication-enablement effort. The roadmap must be used in conjunction with other more detailed Federation documents, many of which are listed in Section 1.4, Document References, and in collaboration with the E-Authentication Program Management Office (PMO).

The roadmap is flexible. Some phases may be executed in parallel. Similarly, some tasks within a phase may be executed in parallel. The PMO collaborates with Potential Federation Members throughout the joining the Federation lifecycle to make such determinations, and to address all other issues and requirements.

The roadmap assumes that initial investigation (e.g., learning about the Federation), deciding whether to participate in the Federation, and signing documents of intention (e.g., Memorandum of Understanding) already have been completed.

Some steps are specific to a type of system implementation (assertion-based, certificate-based) and/or type of Federation Member (credential service provider, relying party). Alerts to that effect are included throughout the document.

A Federation Member may join more than one E-Authentication-enabled service over time. However, the Federation member must follow the process defined herein for each service. The Federation Member may consult with the PMO to identify exceptions to the process because of earlier efforts. The PMO must approve all exceptions.

Table of Contents

Figures

1. INTRODUCTION

Joining the U.S. E-Authentication Identity Federation (Federation) requires success completion of various activities in a particular order. The activities include, but are not limited to, executing agreements, requirements gathering and analysis, implementing technology and support services, assessing compliance, and making E-Authentication-enabled services accessible to end users. This document highlights the flow and relationship of those activities in order to provide a useful, usable methodology for joining the Federation. In doing so, the methodology optimizes and expedites the process, while reducing risk and uncertainty.

The process of joining the Federation is flexible to optimize deployment efficiency. There is flexibility and discretion as to when certain activities can occur, or when scheduling of certain activities can be requested. Such flexibility expedites the process of joining the Federation. For example, some activities can occur in parallel or in a slightly different order. The E-Authentication Program Management Office (PMO) in accordance with the best interests of the Federation makes discretionary decisions.

A Federation Member may join more than one E-Authentication-enabled service over time. However, the Federation member must follow the process defined herein for each service. The Federation Member may consult with the PMO to identify exceptions to the process because of earlier efforts. The PMO must approve all exceptions.

Please read this document prior to other Federation documents. This document provides an important "big picture" context that enhances understanding of other Federation documents.

1.1 Document Organization

This document describes the phased approach Potential Federation Members follow when joining the Federation. Accordingly, the main body of the document is organized by phases. Each phase section highlights the chief steps and processes specific to it. In addition, each phase lists key input, outputs, and milestones. A brief discussion of post-joining responsibilities is included in the Appendix. Finally, essential terms and acronyms are defined.

1.2 Audience and Objective

This document is primarily intended for project managers who are integrating their system with the Federation. The project manager can use this document and associated templates (e.g., project plan) to draft an initial project plan quickly. Other individuals involved in the integration (e.g., management; technical staff; support staff) may also benefit from reviewing this document, as it provides a "big picture" perspective of the entire "Joining the Federation" process from beginning to end.

1.3 Background

As part of the President's Management Agenda, the E-Authentication Initiative enables trust and confidence in E-Government transactions through the establishment of an integrated policy and technical infrastructure for electronic authentication. Through the Federation, citizens and businesses have simpler access to multiple services through the re-use of credentials and established identities.

The management of trust among relying parties (RPs), Credential Service Providers (CSPs) and end users is the essence of the Federation. CSPs are commercial or government entities authorized by the E-Authentication Program Management Office (PMO) to provide credentials (e.g., personal identification numbers (PINs), passwords, X.509 digital certificates) to potential end users for access to Federation Member systems. CSPs are organizations that provide credentials and Credential Services (CSs). RPs are applications, systems or services that rely on (i.e., trust) the CSs of CSPs. End users are people or organizations that have credentials issued by a CSP and desire to use that credential to conduct business with an RP.

To manage the trust relationships, the PMO has implemented a federated architecture that leverages credentials from multiple domains through certifications, guidelines, industry standards adoption, and policies. The federated architecture is the Authentication Service Component (ASC) of the Federal Enterprise Architecture. Currently, the ASC supports two authentication mechanisms that can be implemented by Federation Members:

- Assertion-based authentication via Security Assertion Markup Language (SAML). Assertion-based authentication is typically used for lower assurance levels (e.g., level 1, level 2). Systems within this category are:
    - An RP – relies upon identity assertions issued by the CS to process a transaction or grant access to information or a system.
    - A CS – a service that provides credentials to subscribers for use in electronic transactions. A CS authenticates an end user using an approved authentication mechanism. The CS then issues an identity assertion to the RP.
- Certificate-based authentication via X.509 digital certificates. Certificate-based authentication is typically used for higher assurance levels. Systems within this category are:
    - An RP – authenticates the end user directly, using the X.509 digital certificate presented to it.
    - A CS – a service that issues X.509 digital certificates to end users.

Please review [OMB M-04-04] and [NIST SP 800-63] for greater detail regarding the assurance levels referenced above.

1.4 Document References

The following is a list of documents that will be of interest to the Federation Member during the life cycle of joining the Federation. They provide additional insights, guidance, and requirements. Some documents may be relevant for one task only. Other documents may be relevant in many places.

This document uses National Institute of Standards and Technology (NIST) convention for citing documents. The shorthand format *[Doc Reference]* represents the document referenced in this section. For example, [CAF] is a shorthand reference that refers back to this section's full citation for the *Credential Assessment Framework* document.

[Adopted Scheme]	E-Authentication Federation Adopted Schemes, Version 1.0.0 http://www.cio.gov/eauthentication/TechSuite.htm
[Boarding Memo]	Compliance with Federal Policy required for Boarding Available from the PMO
[Boarding Process]	The E-Authentication Federation Boarding Process Available from the PMO

[CAF] Credential Assessment Framework
http://www.cio.gov/eauthentication/CredSuite.htm

[Change Mgmt FAQ] E-Authentication Change Management FAQs
Available from the PMO

[Data Sheet] Federation Member Data Sheets for RP and CSP
Available from the PMO

[E-Auth Web Site] E-Authentication Federation web site
http://www.cio.gov/eauthentication

[EETP] FPKI OA: End Entity Test Procedures
Available from the PMO

[E-GCA CP] "X.509 Certificate Policy for the E-Authentication Certification Authorities", Version 1.0, September 29, 2004
http://www.cio.gov/fpkipa/documents/EGovCA-CP.pdf

[E-GCA Process] Certificate Life-Cycle Methodology, E-Governance Certificate Authorities
http://cio.gov/eauthentication/documents/EGCAmethodology.pdf

[E-GCA Request] E-GCA Request Generator
Available from the PMO

[E-GCA Video] E-GCA Certificate Request Video Instructions
Available from the PMO

[E-RA] Electronic Risk and Requirements Assessment
http://www.cio.gov/eauthentication/era.htm

[Escalation Plan] E-Authentication Escalation Plan
Available from the PMO

[Escalation POC Form] Escalation Points Of Contact Spreadsheet template
Available from the PMO

[FBCA] Federal Bridge Certification Authority
www.cio.gov/fbca

[FISMA] Federal Information Security Management Act http://csrc.nist.gov/sec-cert/

[FMD] E-Authentication Federation Membership Documents
http://www.cio.gov/eauthentication/MembershipDocuments.htm

[FMD Agreement] Federation Membership Documents; Agreements for RPs and CSPs
http://www.cio.gov/eauthentication/MembershipDocuments.htm

[FMD Memo] Compliance with E-Authentication Identity Federation Membership Documents
Available from the PMO

[FPKIPA Web Site] Federal Public Key Infrastructure Policy Authority web site
http://www.cio.gov/fpkipa/

[Governance] E-Authentication Federation Governance
http://www.cio.gov/eauthentication

[IdM Case Study] E-Authentication Identity Management Services Case Study
Contact the PMO for a copy

[Interface Spec] E-Authentication Federation Architecture 2.0 Interface Specifications
http://www.cio.gov/eauthentication/TechSuite.htm

[Lab Test Plan] E-Authentication Lab Test Plan
Available from the PMO

[Lab Wiki] E-Authentication Lab Test Wiki
http://kasparov.eauth.enspier.net/tiki/tiki-index.php

[NIST SP 800-63] Electronic Authentication Guideline, National Institute of Science and Technology (NIST Special Publication 800-63)
http://csrc.nist.gov/publications/nistpubs/

[Node Testing] E-Authentication Node Connection Testing Instructions
Available from the PMO

[OMB M-03-22] OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Office of Management and Budget (OMB) Memorandum M-03-22
http://www.whitehouse.gov/omb/memoranda/m03-22.html

[OMB M-04-04] E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) Memorandum M-04-04
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[Operational Standards] E-Authentication Federation Operational Standards
http://www.cio.gov/eauthentication

[Prereq Checklist] The E-Authentication Testing Prerequisites and Checklist
(one for RP, one for CS)
Available from the PMO

[Project Plan Template] E-Authentication Project Templates for CSP and RP
Available from the PMO

[Rollout Checklist] Relying Party Rollout Checklist
Available from the PMO

[SAML Products] The Approved E-Authentication Technology Provider List
http://cio.gov/eauthentication/documents/ApprovedProviders.htm

[Selecting Technology] Selecting an Approved Technology
http://www.cio.gov/eauthentication/documents/SelectApprovedTechnology.pdf

[Style Guide] E-Authentication Style Guide
All available from the PMO

[Tech Approach] Technical Approach for the Authentication Service Component, Version 2.0.0
http://www.cio.gov/eauthentication/TechSuite.htm

[Tech Suite] E-Authentication Technical Architecture suite of documents
http://www.cio.gov/eauthentication/TechSuite.htm

[Test Harness] E-Authentication Lab Test Harness
http://kasparov.eauth.enspier.net/samlharness/ui

[User Activation] Relying Party User Activation Within E-Authentication
Available from the PMO

[User Experience] E-Authentication User Experience: Screenshots and Process Flows
Available from the PMO

[Validation Products] Qualified Validation List
http://www.cio.gov/fbca/validation_solutions.htm

[Validation Options] E-Authentication PKI Certificate Validation Options
Available from the PMO

[Validation Reqmnts] Functional Requirements for Path Validation Systems
Available from the PMO

[Waiver Form] Waiver Request Form
Available from the PMO

[Waiver Q&A] E-Authentication Federation Waivers Questions and Answers
Available from the PMO

2. Joining the Federation Phases

This document presents the "phased roadmap" to joining the Federation. The roadmap encapsulates and organizes all activities that occur during the process. The roadmap is flexible. Some phases may be executed in parallel. Similarly, some steps within a phase may be executed in parallel. The PMO collaborates with Potential Federation Members throughout the joining the Federation lifecycle to make such determinations, and to address all other issues and requirements.

The phased approach assumes that initial investigation (e.g., learning about the Federation), deciding whether to participate in the Federation, and signing documents of intent (e.g., Memorandum of Understanding) are completed.

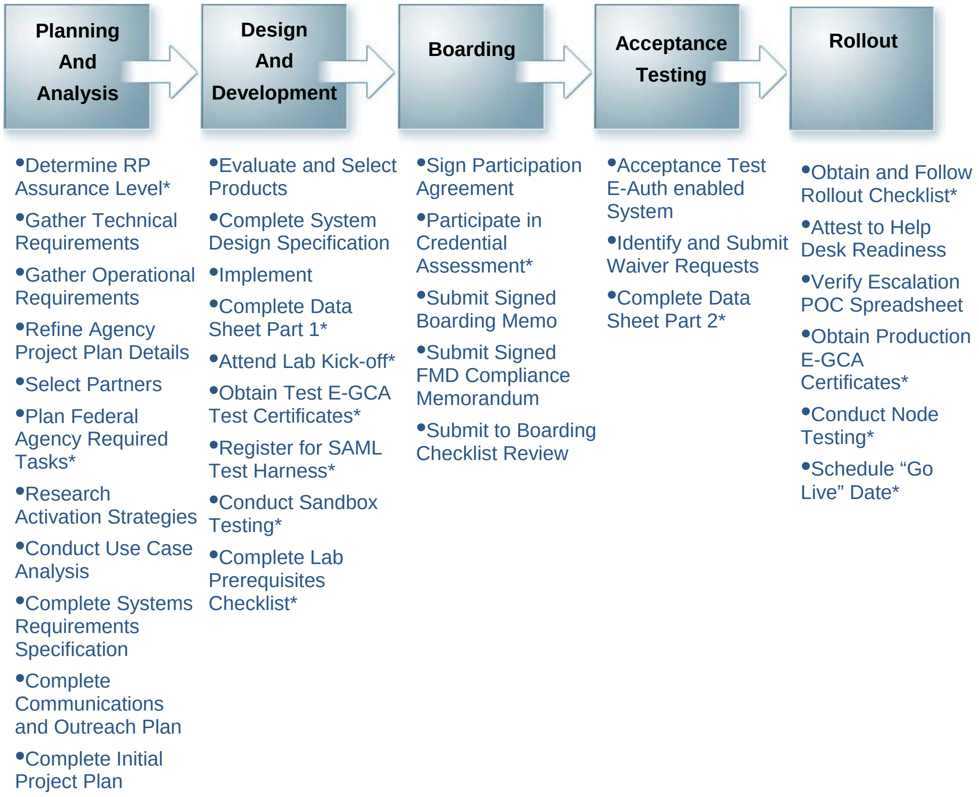
Note that some steps are specific to a type of system implementation and/or type of Federation Member. Throughout phase discussions, annotations indicate type-specific steps. Annotated steps should be done only if applicable. An item not annotated applies to everyone. The type-specific annotations are:

• Assertion-based	Assertion-based Only
• Certificate-based	Certificate-based Only
• RP	RP Only
• CSP	CSP Only
• Federal Agency	Federal Agency Only

The following sections address each phase and their applicable activities.

Figure 2-1 illustrates the full life cycle of joining the Federation. Each phase specifies key activities to be completed. Items marked with an asterisk are type-specific (e.g., assertion-based vs. certificate-based, RP vs. CSP).

Figure 2-1 Phases of Joining the Federation



Planning And Analysis

- Determine RP Assurance Level*
- Gather Technical Requirements
- Gather Operational Requirements
- Refine Agency Project Plan Details
- Select Partners
- Plan Federal Agency Required Tasks*
- Research Activation Strategies
- Conduct Use Case Analysis
- Complete Systems Requirements Specification
- Complete Communications and Outreach Plan
- Complete Initial Project Plan

Design And Development

- Evaluate and Select Products
- Complete System Design Specification
- Implement
- Complete Data Sheet Part 1*
- Attend Lab Kick-off*
- Obtain Test E-GCA Test Certificates*
- Register for SAML Test Harness*
- Conduct Sandbox Testing*
- Complete Lab Prerequisites Checklist*

Boarding

- Sign Participation Agreement
- Participate in Credential Assessment*
- Submit Signed Boarding Memo
- Submit Signed FMD Compliance Memorandum
- Submit to Boarding Checklist Review

Acceptance Testing

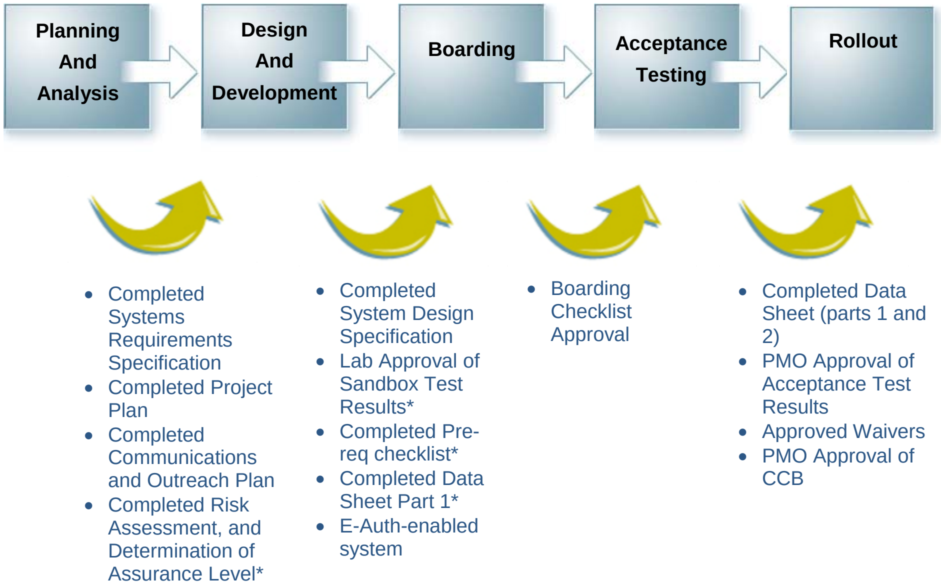
- Acceptance Test E-Auth enabled System
- Identify and Submit Waiver Requests
- Complete Data Sheet Part 2*

Rollout

- Obtain and Follow Rollout Checklist*
- Attest to Help Desk Readiness
- Verify Escalation POC Spreadsheet
- Obtain Production E-GCA Certificates*
- Conduct Node Testing*
- Schedule “Go Live” Date*

Figure 2-2 highlights the key events that trigger transition from one phase to another. Items marked with an asterisk are type-specific.

Figure 2-2 Phase Transition Triggers



- Completed Systems Requirements Specification
- Completed Project Plan
- Completed Communications and Outreach Plan
- Completed Risk Assessment, and Determination of Assurance Level*

- Completed System Design Specification
- Lab Approval of Sandbox Test Results*
- Completed Pre-req checklist*
- Completed Data Sheet Part 1*
- E-Auth-enabled system

- Boarding Checklist Approval

- Completed Data Sheet (parts 1 and 2)
- PMO Approval of Acceptance Test Results
- Approved Waivers
- PMO Approval of CCB

3. Planning and Analysis Phase

The Planning and Analysis phase should be executed with a number of primary goals in mind to achieve successful E-Authentication enablement (Enablement). Foremost, an understanding of the E-Authentication project lifecycle and technical architecture should be reached. This requires familiarity with all applicable facets of Enablement such as, but not limited to activation, use cases, E-Governance Certification Authorities (E-GCA) certificates, and interface specifications. Finally, a thorough systems requirements gathering process, which accounts for the above elements, must be performed.

An additional consideration during this phase is whether to implement an enterprise-wide (i.e., organizational-wide) approach to E-Authentication, rather than integrating individual applications. Integrating a single enterprise-wide identity management service (IdM Service) with the Federation can provide considerable benefits to the organization. For example, IdM Services consolidate and standardize authentication and policy enforcement of many applications within an organization. Consequently, IdM Services have the most benefit for Federation Members with multiple applications requiring authentication.

3.1 Phase Inputs

Inputs to this phase include, but are not limited to the following:

- [Tech Suite]
- [FMD]
- [Style Guide]
- [Boarding Process]
- [Project Plan Template]
- [FISMA]
- [User Activation]

3.2 Phase Tasks

3.2.1 Complete Initial Project Plan

A project plan is necessary to communicate project Enablement tasks and milestones to the PMO and other Federation members. In addition, the project plan helps the Potential Federation Member track the overall progress of the effort throughout the lifecycle of the effort. The project plan conveys project metrics and scheduling timelines to the PMO for review. The Potential Federation Member should use [Project Plan Template] to jumpstart the process. [Project Plan Template] reflects best practices established through the analysis of previous Federation deployments. At this stage, an initial project plan should be drafted, with the intent to complete it by phase-end.

Milestone: Initial project plan prepared and delivered

3.2.2 Gather Technical Requirements

The Potential Federation Member should gather and analyze technical requirements specific to their Enablement effort. Technical requirements gathering may include, but is not limited to the following:

- End user flow
- Technical interoperability
- Network security
- Activation

- Landing page
- Risk mitigation

Milestone: Identification of applicable technical requirements

3.2.3 Gather Operational Requirements

The Potential Federation Member should gather and analyze technical requirements specific to their Enablement effort. Operational requirements gathering includes, but is not limited to the following:

- Helpdesk
- Transaction and audit logging
- Checking and updating server credentials
- Business continuity
- Security rules to open ports
- FISMA

For additional information, refer to [Operational Standards] and [Governance]. The standards defined in those documents leverage federally mandated standards and commercial best practices, ensuring that the best interests of the Federation, particularly operating environment integrity, are maintained.

Milestone: Identification of applicable operational requirements

3.2.4 Plan for Boarding

Boarding requires executing various agreements, declaring compliance with several government-wide policies, and meeting Federation architecture and technical interface requirements. [Boarding Process] includes a checklist of items that must be completed. These items ensure that Federation requirements have been met. Successful boarding is required prior to moving into the acceptance testing phase.

The Potential Federation Member should become familiar with the boarding process as soon as possible. The boarding checklist and boarding compliance memos ([FMD Memo], [Boarding Memo]) should be reviewed in detail. Impacts to business processes should be identified and analyzed. Legal review of checklist items should be scheduled as necessary.

3.2.5 Determine Assurance Level RP Only

The government has outlined four levels of identity assurance per guidance from [OMB M-04-04]. As the System Owner, you must assess the level of risk (i.e., level of identity assurance) you are willing to accept for your RP. Risk refers specifically to the risk of a false positive authentication (i.e., the risk of someone successfully claiming to be someone they are not). The risk assessment should consider potential impacts in the case of an authentication error, as outlined in OMB M-04-04. The Electronic Risk and Requirement Assessment (E-RA) tool can be of assistance in determining level of risk and assurance level. Internal risk assessments based on [OMB M-04-04] may be used to assess risk and assurance level.

Milestone: Determination of Assurance Level

3.2.6 Select Initial Federation Member Partner(s)

The Potential Federation Member should select the RP(s) or CSP(s) they expect to federate with in the production environment. This decision should be reached after an evaluation of business and technical factors (e.g., community of interest, ability to technically interoperate, receivable or available optional attributes). The PMO assists the Potential Federation Member in the following ways:

- Assessing the needs of the RP's end users
- Identifying CSP(s) that will provide the most benefits to the RP's end users
- Identifying CSP(s) that can technically interoperate (i.e., compatible) with the RP

Milestone: Selected RP or CSP Partner(s)

3.2.7 Plan Federal Agency Specific Tasks

Federal Agency Only

In addition to planning for agency-specific requirements, a Potential Federation Member that is a federal agency must also plan for specific federal government requirements to which they must comply. The Boarding phase formal assessment verifies successful completion of these activities. Federal government requirements include, but are not limited to the following:

- Privacy Impact Assessment (PIA)
- System of Records Notice (SORN) if required by PIA
- Section-508 Compliance
- FISMA Authority to Operate (Certification and Accreditation)
- Paperwork Reduction Act

Milestone: Completed Federal Requirements

3.2.8 Identify Activation Strategy

RP Only

The RP activates an end user when the end user's subject name (in the SAML assertion or in the PKI certificate) is unrecognized. This is because in a federated environment, each CS and Certification Authority (CA) has a different subject name for the same end user, to guarantee Federation-wide uniqueness. There are four approaches to activation: automatic, prompted, deferred, and no activation. [User Activation] provides additional information.

The Potential Federation Member should review and analyze viable activation strategies. [User Activation] should be read for an initial overview, and an understanding of pros and cons associated with each alternative. After careful consideration of alternatives vis a vis objectives and constraints, one or more activation strategies should be identified.

Milestone: Activation Strategy Identified

3.2.9 Identify Credentialing Processes for E-Authentication Customers CSP Only

The CS must identify repeatable processes for credentialing its E-Authentication customers. Although an existing process may exist for user credentialing, the CS may wish to develop new processes to address the needs of its E-Authentication customers. One consideration that may drive the development of new processes is the need to collect and identify which optional attributes will be available to RP partners.

Milestone: User Credentialing Processes Identified

3.2.10 Conduct Use Case Analysis Assertion-based Only

Within the ASC, an end user can interact directly with RPs, CSs, and possibly an external site. [Tech Approach] details the various use cases. The Potential Federation Member must plan for these different use cases as applicable. Use case analysis may indicate the need for design changes to support a friendly end user approach. One example is possible business process reengineering of the user registration process.

Milestone: Identification of Applicable Use Cases and Associated Technical Requirements

3.2.11 Complete System Requirements Specification

Three elements make up a comprehensive systems requirements specification:

- Functional Requirements
- Technical Requirements
- Operational Requirements

Functional requirements encompass use case flows – primarily defined in [Tech Suite] and [User Activation].

Technical requirements encompass the system requirements for integrating the application into the ASC – primarily defined in [Tech Suite].

Operational requirements encompass Federation business processes and support – primarily defined in [FMD]. These requirements may include, but are not limited to helpdesk, escalation, and business continuity

Milestone: Completed System Requirements Specification

3.2.12 Develop Communications and Outreach Plan

The Potential Federation Member should develop a plan that notifies end users of the impending federated approach. The plan should address end user awareness, changes to business processes, collateral materials, and end user support.

Milestone: Completed Communications and Outreach Plan

3.2.13 Update Project Plan

The initial project plan must be revised and extended to reflect the planning and analysis activities of this phase. Updating of the project plan shall be a recurring milestone throughout the project life cycle. These updates are necessary to communicate the correct milestones to the PMO and assist in coordination and scheduling with other Federation Members, Operations, the Interoperability Lab (Lab), and the E-Authentication Help Desk.

Milestone: Revised Project Plan

3.3 Phase Outputs

Upon completion of the Planning & Analysis phase, the following documents should be considered phase outputs or milestones necessary for moving into the next phase.

- Updated Project Plan
- Completed Risk Assessment RP Only
- Completed Systems Requirements Specification
- Completed Communications and Outreach Plan

4. Design and Development Phase

Potential Federation Members design, document, and develop their system during this phase. Issues to address include, but are not limited to technical interoperability, commercial-off-the-shelf (COTS) product selection, exception handling, landing pages, redirecting unauthenticated end users, end user interface (UI), and activation. Potential Federation Members should develop user interface and flow diagrams that identify the process and screens the end user will encounter when using the system. The Potential Federation Member must conduct testing against applicable Federation requirements as appropriate. In addition, Potential Federation Members should conduct backend testing to ensure that internal systems are not affected by the E-Authentication-enabled system.

4.1 Phase Inputs

Inputs to this phase include, but are not limited to the following:

- Project Plan
- System Requirements Specification
- [Tech Suite]
- [Approved Products]
- [User Activation]
- [Style Guide]
- [Prereq Checklist] Assertion-based Only
- [E-GCA Process] Assertion-based Only
- [Lab Test Plan] Assertion-based Only
- [CAF Suite] CSP Only
- [Validation Options] Certificate-based Only RP Only
- [Validation Reqmnts] Certificate-based Only RP Only

4.2 Phase Tasks

4.2.1 *Evaluate and Select Products*

Those wishing to participate in the Federation must use technology that has demonstrated the ability to support the Federation technical architecture. The PMO publishes [SAML Products] and [Validation Products] from which Potential Federation Members may select product(s) that support their Federation adopted scheme. Some products may consist of a suite of tools. Depending upon the Potential Federation Member's requirements, the entire product suite may be appropriate and/or may enable value-added functionality. Potential Federation Members may implement their own solution in lieu of a product under limited circumstances and with PMO approval. In these instances, Potential Federation Members must accept full responsibility for the increased risk introduced to the project deployment based on the use of an unapproved product. See [Selecting Technology] for more information.

Milestone: Selection and Procurement of Technology Product(s)

4.2.2 *Complete System Design Specification*

The System Design Specification (SDS) should address all issues relevant to the design of the Potential Federation Member's architecture. The document should determine how Federation use cases will be implemented. The design should also incorporate the process flows of the user interface, landing page, exception handling, and activation. Section-508 compliance and Federation branding requirements should also be considered. Issues specific to the authentication mechanism should be addressed as appropriate (e.g., validation and hint list for certificate-based, SAML technical interoperation for assertion-based).

The Potential Federation Member shall submit the completed SDS to the PMO for review. The PMO provides comments based on the best practices derived from previous Federation deployments.

Milestone: System Design Specification

4.2.3 Implement E-Authentication Enabled System

The Potential Federation Member enables their system in accordance with the SRS and SDS. The objective is to implement what was planned in the prior phase – in the spirit of a "plan, do, check, act, adjust" methodology. Implementation is not just coding. It includes business-related tasks, policy-related tasks, and other tasks that need to be completed such as, but not limited to screen flow approvals, technical reviews, software builds, or other configuration tracking processes to ensure completeness and compliance to the SRS.

Milestone: E-Authentication Enabled System

4.2.4 Attend Lab Kickoff Meeting Assertion-based Only

The Lab kickoff meeting introduces the Potential Federation Member to their assigned Lab Engineer, and discusses the technical services offered by the Lab. These services are Federation architecture technical support, review of sandbox testing, and acceptance testing of the E-Authentication-enabled system. Technical support entails assistance with Federation deployment. The purpose and activities conducted during acceptance testing are also discussed during this meeting.

Milestone: Understanding of Lab Role and Identification of Lab Engineer

4.2.5 Complete Data Sheet Part 1

The information on the [Data Sheet] is used throughout the project lifecycle. The data sheet provides information about the application joining the Federation. The section titled "Part I" is the functional information section, and includes information such as points of contacts, assurance level, additional project scope information, and a brief description of the application.

Milestone: Completed Data Sheet Part 1

4.2.6 Conduct Sandbox Testing Assertion-based Only

Sandbox Testing allows a Potential Federation Member to configure and test their E-Authentication-enabled system in an informal environment with the assistance of a Lab Engineer. Sandbox testing may begin as soon as a Potential Federation Member has acquired their approved product. The following sections discuss preparation steps. Figure 4-1 highlights the high-level sandbox testing process.

4.2.6.1 Connect to SAML Test Harness

The [Test Harness] is an automated testing tool available to Potential Federation Members. It may be used without direct Lab support and is available during non-business hours. It also provides detailed logs, which can be used for debugging and configuration tasks.

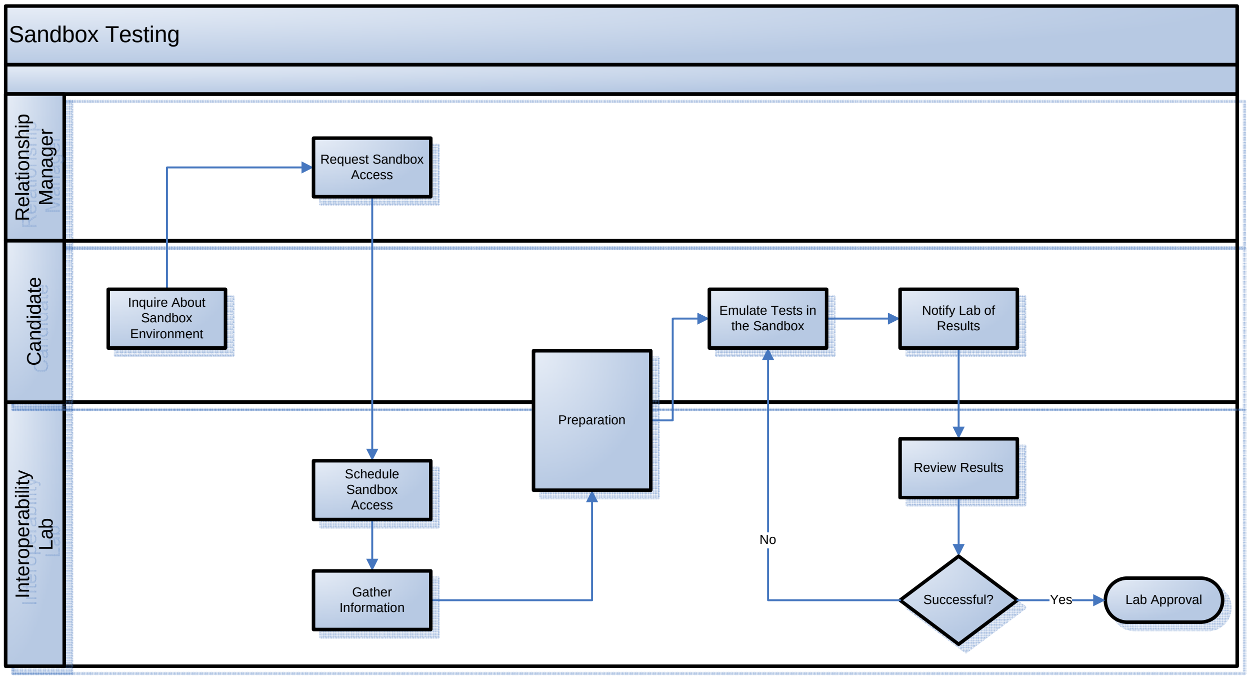
Milestone: SAML Test Harness Connection and Use

4.2.6.2 Obtain Test E-GCA Certificate(s)

Test E-GCA certificate(s) are required to begin interoperability testing with the Lab. The Potential Federation Member must request the certificate(s) from their assigned Lab Engineer. The E-GCA Test CA issues the certificate(s), which are installed on the appropriate system. [E-GCA Process] details the E-GCA certificate request and issuance process. See also [E-GCA Request] and [E-GCA Video].

Milestone: Obtained Test E-GCA Certificate(s)

Figure 4-1 Sandbox Testing Process



The Lab verifies Sandbox Testing completion during the Pre-Acceptance Testing stage and has the Potential Federation Member fill out and return [Prereq Checklist]. This document attests that the necessary tasks have been completed in order to move forward to Acceptance Testing. These tasks typically include full interoperability with all approved products and other requirements verified during Acceptance Testing.

Milestone: Verified Completion of Sandbox Testing

Milestone: Verified Sandbox Testing Pre-requisites Checklist

4.3 Phase Outputs

Upon completion of the Design & Development phase, the following documents should be considered phase outputs or milestones necessary for moving into the next phase.

- Completed System Design Specification
- Completed Data Sheet Part 1
- E-Authentication Enabled System
- Verified Sandbox Testing Pre-requisites Checklist Assertion-based Only
- Test E-GCA Certificate(s) Assertion-based Only

5. Boarding Phase

During the Boarding Phase, the Potential Federation Member completes all remaining boarding checklist tasks and verifies with the PMO that they have been completed. Completion of the checklist ensures that the Potential Federation Member has met Federation governance, business, and operational requirements. Upon successful boarding, the Potential Federation Member becomes a Federation Member. Boarding approval is a firm pre-requisite for transition to Acceptance Testing phase

5.1 Phase Inputs

Inputs to this phase include, but are not limited to the following:

- [Boarding Process]
- [Boarding Memo]
- [FMD Memo]
- [FMD Agreement]
- [CAF] CSP Only

5.2 Phase Tasks

5.2.1 *Participate in Credential Assessment* CSP Only

A CSP must participate in a credential assessment to determine the assurance level of the credentials of the proposed CS. A successful credential assessment assures compatible Federation RPs as to the veracity, and thus dependability, of the proposed credential. This is essential for Federation-wide trust. The assessment is conducted in accordance with [CAF], which defines a consistent, structured process and criteria. [CAF] is based upon [OMB M-04-04] and [NIST SP 800-63].

The Federation defers governance of public key certificates to the Federal Public Key Infrastructure Policy Authority (FPKIPA). FPKIPA approval of cross-certification means all current Federation requirements have been met by the Potential Federation Member certificate-based CS, for a designated Federation assurance level. No additional criteria are required. A certificate-based CS that has not had their policies mapped by the FPKIPA cannot be assessed. See [FPKIPA Web Site] for details.

An assertion-based CSP should expect the following process:

- Submit application for assessment
- Submit assessment package
- Schedule assessment
- Participate in CS assessment
- Obtain assessment report
- Obtain determination of assurance level

A certificate-based CSP should expect the following process:

- Submit proof of FPKI cross-certification
- Obtain determination of assurance level from FPKIPA

Milestone: Credential Assessment Approval

5.2.2 Sign Federation Participation Agreement

[FMD Agreement] establishes the legal agreement for participation in the Federation. It incorporates by reference other documents such as [Governance] and [Operational Standards]. Someone capable of committing the organization to the Federation must sign the agreement.

Milestone: Signed Federation Participation Agreement

5.2.3 Provide Signed FMD Memo Attestation

By submitting [FMD Memo], the Federation Member attests that they are currently compliant with applicable standards in [Governance] and [Operational Standards]. The System Owner or Application Owner must sign the FMD Memo.

Milestone: Submission of Signed FMD Memo

5.2.4 Provide Signed Boarding Memo

By submitting [Boarding Memo], the Federation Member attests that they are currently compliant with the government information system requirements detailed in Section 3.10. The Federation Member's Designated Approving Authority (DAA) must sign this document.

Milestone: Submission of Signed Boarding Memo

5.2.5 Submit to Boarding Checklist Review

The Potential Federation Member must complete all Boarding phase activities before the PMO reviews the boarding checklist for completeness and correctness. The PMO verbally communicates boarding checklist approval via email or status meeting. Approval indicates:

- The Potential Federation Member is now a Federation Member
- The Federation Member is officially "boarded"
- The Federation Member can proceed to Acceptance Testing

Milestone: PMO Approval of Boarding Checklist

5.3 Phase Outputs

Upon completion of the Boarding phase, the following documents should be considered phase outputs or milestones necessary for moving into the next phase.

- Signed Participation Agreement
- CAF Approval CSP Only
- Approved Boarding Checklist

6. Acceptance Testing Phase

Acceptance testing ensures that a Federation Member's system is compliant with all applicable Federation specifications and requirements. The acceptance testing approach differs between assertion-based systems and certificate-based systems. The Lab conducts assertion-based system acceptance testing, with Federation Member assistance as necessary. The Federation Member conducts certificate-based system acceptance testing using test procedures available from the PMO.

6.1 Phase Inputs

Inputs to this phase include, but are not limited to the following:

- E-GCA Test Certificates Assertion-based Only
- Verified Sandbox Testing Assertion-based Only
- [EETP] Certificate-based Only

6.2 Phase Tasks

6.2.1 Complete Data Sheet Part 2

[Data Sheet] Part 2 provides information to the Lab, PMO, or the Federation Operations Center required for the Federation Member's system to go-live. The Federation Member must complete [Data Sheet] Part 2 during the Acceptance Testing Phase and submit it to the PMO for review. Complete Data Sheet Part 2 as early as possible in this phase so as not to delay the Rollout phase.

Milestone: Completed Data Sheet Part 2

6.2.2 Submit to Lab Testing Assertion-based Only

The Lab conducts Acceptance Testing, usually with minimal involvement from the Federation Member. Acceptance Testing ensures compliance with the applicable interface specification documented in [Interface Spec], and interoperability with all other approved products. The Lab uses a formal test plan and produces a Test Report. All testing must be conducted in a production-ready environment to ensure the transition to production is as smooth as possible. The Lab issues an Acceptance Test Report (Report) to the PMO. The Report summarizes findings, including deficiencies, and provides a Pass/Fail recommendation. After evaluating the Test Report, the PMO makes the final Pass/Fail decision, but first may request additional testing. The PMO notifies the Federation Member of the final decision.

Milestone: Successful Lab Acceptance Testing

6.2.3 Conduct Certificate-based Testing

Certificate-based Only RP Only

End entity test procedures (EETP) are required to test certificate-based RP systems not using a Federation Managed Validation and Translation Service (MVTS). The Federation Member must obtain end entity test certificates from the PMO prior to testing. The Federation Member should test the validation mechanism it has implemented (e.g., path discovery and validation (PDVal), Trust List). Certain parts of the EETP apply to PDVal and other parts of the EETP apply to Trust List. The Federation Member submits a Test Report to the PMO for review and approval. The PMO may request follow-up testing. The PMO communicates end entity testing approval. If using a MVTS, the Federation Member should coordinate and test with the PMO and MVTS provider.

Milestone: Successful Certificate-based Testing

6.2.4 Identify and Obtain Waivers

If necessary, the Federation Member should create Governance and Operational Standards waiver requests and submit them to the PMO using [Waiver Form]. A waiver may be necessary for technical, financial, or other reasons. Only the PMO may initiate deployment (product) waivers. The PMO issues waivers on a case-by-case basis. [Waiver Q&A] provides additional information regarding the waiver process.

Milestone: Waiver Requests Submitted

6.3 Phase Outputs

Upon completion of the Acceptance Testing phase, the following documents should be considered phase outputs or milestones necessary for moving into the next phase.

- Acceptance Test Report Assertion-based Only
- Completed EETP Certificate-based Only
- Waivers Approved by the PMO
- Completed Data Sheet

7. Rollout Phase

The Rollout phase may begin only when Acceptance Testing and Boarding are successfully completed. In this phase, the Federation Member completes tasks necessary for production support, and the Change Control Board (CCB) reviews and approves the change proposal officially requesting that the Federation Member system be added to the production ASC. In addition, assertion-based systems conduct node connection testing in the production ASC to ensure proper technical interoperability with partner Federation Member systems. From an operational standpoint, Federation Member systems are called ‘nodes’.

7.1 Phase Inputs

Inputs to this phase include, but are not limited to the following:

- Boarding Approval
- [Data Sheet]
- [Node Testing] Assertion-based Only
- [Rollout Checklist] Assertion-based Only RP Only
- [Escalation POC Form]
- [Escalation Plan]

7.2 Phase Tasks

7.2.1 *Support Change Proposal Submittal to Change Control Board (CCB)*

The PMO submits the change proposal (CP) on behalf of the Federation Member. The Federation Member must complete Data Sheet Parts 1 and 2 prior to the CCB. The CCB is the governance entity empowered to review and approve changes to the production ASC. The CP is the official request to allow the Federation Member system to integrate into and operate in the production ASC.

Milestone: Approved Change Proposal

7.2.2 *Obtain Production E-GCA Certificates* Assertion-based Only

Upon CCB approval, the PMO sends a Letter of Authorization (LOA) to the FPKI OA on behalf of the Federation Member. The LOA authorizes the PKI OA to issue production E-GCA certificate(s) to that Federation Member, as appropriate. In parallel and out-of-band, the Federation Member submits a Public Key Cryptography Standards (PKCS) #10 Production Certificate Request to the FPKI OA with the Server Certificate Request Form.

Upon receiving the LOA and PKCS #10 Production Certificate request, the FPKI OA generates the production E-GCA certificate(s) and issues them to the Federation Member. The Federation Member receives the production certificate(s) out of band, and receives a shipping tracking number from the FPKI OA. Upon receipt, the Federation Member adds the production certificate(s) to its metadata file. Production certificate issuance may take one to two (1-2) weeks after CCB approval. [E-GCA Process] details the E-GCA certificate request and issuance process.

Milestone: Obtained Production E-GCA Certificate(s)

7.2.3 Complete Relying Party Rollout Checklist Assertion-based Only RP Only

The Federation Member completes the [Rollout Checklist] in preparation for Node Connection Testing. Some key steps included within the Checklist are the creation of signing and encryption certificate requests for submittal to the E-GCA and the creation of [Interface Spec] compliant metadata.

Milestone: Completed Relying Party Rollout Checklist

7.2.4 Verify Escalation POC Spreadsheet

The PMO maintains an Escalation POC Spreadsheet used by the Help Desk when an issue arises. The PMO obtains the POC information from the Federation Member's Data Sheet. During the Rollout phase, the PMO asks the Federation Member to confirm that each Escalation POC is current and correct. The Federation Member is responsible for communicating future POC changes to the PMO via an email

Milestone: PMO Email Verifying the Escalation POC Spreadsheet

7.2.5 Attest to Federation Member Help Desk Readiness

The Federation Member must attend an E-Authentication Support Services Meeting. In this meeting, the PMO discusses support services offered by the PMO and related documentation available from the PMO.

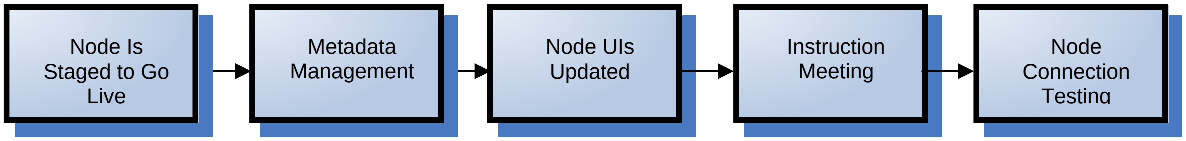
The Federation Member must also attest that they have established and trained a help desk to support end-users of their Federation Member system. The attestation is sent via an email from the Federation Member's project lead to their Relationship Manager (RM).

Milestone: Help Desk Attestation Email to RM

7.2.6 Conduct Node Connection Testing Assertion-based Only

The Federation Member deploys its Enabled system to its production environment and conducts Node Connection Testing. Testing verifies that end user hand-offs occur properly between connected nodes and authentication is successful. During testing, existing nodes to which the new node is connected continue to perform live transactions; there is no disruption to production service. Figure 7-1 highlights the node connection test process.

Figure 7-1 Node Connection Test Process



7.2.6.1 Stage Node into Production Environment

The Federation Member deploys its Enabled system to its production environment as a new node. In general, the System Owner or System Owner's designee hosts and operates Federation Member systems. Federation Member systems are not hosted or operated by the Federation.

Milestone: Federation Member System Staged into its Production Environment

7.2.6.2 Exchange and Configure Metadata

Prior to connection testing, connected Federation Members exchange signed metadata files through the PMO, who facilitates the exchange. Each Federation Member then configures its node with the others' metadata. Metadata facilitates proper processing (e.g., end user redirects, message signature and validation, message encryption) between nodes.

Milestone: Federation Member provides production Metadata to the PMO

Milestone: Federation Member Configures its System with Metadata from Connected Members

7.2.6.3 Update Node User Interface

If not yet completed, the Federation Member updates the new node's user interface per [Style Guide]. This may include, but is not limited to the Federation logo, Partner logos, and Federation narrative.

Milestone: Federation Member node updated per [Style Guide]

7.2.6.4 Participate in Testing Instructions Meeting

Upon successful metadata exchange and configuration, RM disseminates node connection testing instructions to Federation Members that are in the testing group. The RM then conducts a conference call with the testing group to discuss the instructions and schedule testing.

Milestone: Test Instruction Meeting Completed

7.2.6.5 Node Connection Testing

The Federation Member executes rollout testing until successful completion. Upon successful completion, the parties that were tested must send an email to the RM confirming successful node connection testing. Subsequently the PMO sends the Federation Member a "Welcome to the Federation" email specific to the Federation Member system approved for integration.

Milestone: Successful Deployment of Enabled System

7.2.7 Schedule Production Go-Live Date Assertion-based Only

Upon successful node connection testing, the Federation Member coordinates a go-live date with applicable others in order to ensure Member links are displayed according to [Style Guide].

7.3 Phase Outputs

- Completed Relying Party Roll Out Checklist
- Help Desk Readiness Attestation
- Verified Escalation POC Spreadsheet
- CCB-approved Change Proposal
- Production E-GCA Certificate(s) Assertion-based Only
- Completed Node Connection Testing Assertion-based Only
- Scheduled Go-live Date Assertion-based Only

APPENDIX A: POST ROLLOUT RESPONSIBILITIES

A Federation Member's responsibilities do not end upon successfully joining the Federation. A Federation Member must comply with various ongoing operational requirements, which include, but are not limited to the following:

- **Modifying Your Application Uniform Resource Locator (URL)** – notify Federation Help Desk in advance if the URL for your system is going to be changed.
- **Technology Updates** – ensure that any technology updates or environment changes comply with Federation requirements.
- **Branding Related Updates** – notify the PMO in advance of any branding changes.
- **Audits by the Federation** – support Federation-requested audits as required/requested by the Federation.
- **Reporting** – ongoing reporting of specific operational statistics and activities, as well as notifications of proposed modifications that may negatively impact a Federation Member's interoperability or overall security posture.

See [FMD] for a complete listing of ongoing Federation Member responsibilities. Also, see the [Change Mgmt FAQ] for information regarding modifications to a production system.

APPENDIX B: ACRONYMS

Acronym	Abbreviation For
ASC	Authentication Service Component
ATO	Approval to Operate
CA	Certification Authority
CAF	Credential Assessment Framework
CCB	Change Control Board
CD	Compact Disc
COTS	Commercial Off The Shelf
CP	Certification Policy
CS	Credential Service
CSP	Credential Service Provider
DAA	Designated Approving Authority
EETP	End Entity Test Procedures
E-GCA	E-Government Certification Authorities
E-RA	Electronic Risk and Requirements Assessment
FMD	Federation Membership Documents
FPKI OA	Federal Public Key Infrastructure Operational Authority
FPKIPA	Federal Public Key Infrastructure Policy Authority
GSA	General Services Administration
IdM	Identity Management
LOA	Letter of Authorization
MVTS	Managed Validation and Translation Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PDVal	Path Discovery and Validation
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PMO	E-Authentication Program Management Office
POC	Point of Contact(s)
RP	Relying Party
RM	Relationship Manager
SAML	Security Assertion Markup Language
SDS	System Design Specification
SOP	Standard Operating procedures
SORN	System of Records Notice

Acronym	Abbreviation For
SRS	Systems Requirements Specification
UI	User Interface
URL	Uniform Resource Locator