E-Authentication Interoperability Lab Concept of Operations

Version 1.0.0
July 30, 2004

Executive Summary

The document describes the operation concepts of the E-Authentication Interoperability Lab (Lab). The Lab tests products and solutions for conformance to E-Authentication's Interface Specifications, which are a subset of industry standards. Additionally the Lab tests products for interoperability with other products that purport the same conformance.

Table of Contents

1 Introduction

1.1 Identification

This Concept of Operations (ConOps) document is a high-level description of the E-Authentication Interoperability Lab operation. This document is complemented by The E-Authentication Interoperability Lab Operations Manual, which provides details and guides the Lab personnel on proper daily operations of the Lab.

The concepts discussed herein only apply to the E-Authentication Interoperability Lab (Lab) and not E-Authentication in general.

1.2 Purpose

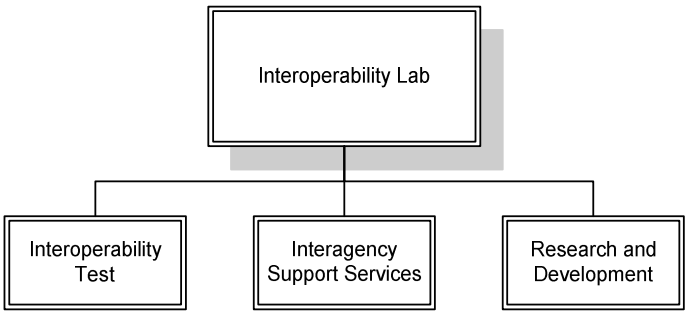
The purpose of this ConOps is to describe the background, general philosophy, organizational operations and support for the Lab. Strict adherence to these concepts will result in consistent selection and testing of products, as well as unbiased test results. The basic premise of this concept is to raise awareness and usability of the Lab, and to meet consistency and timeliness demands of federal and vendor communities.

The E-Authentication Program Management Office (PMO) will consider and approve changes to this ConOps.

1.3 E-Authentication Interoperability Lab

The core function of the Lab is to analyze, test and certify the interoperability of products and systems that desire to participate in E-Authentication. The Lab is a unit of the E-Authentication Initiative and is sponsored by the GSA with participation by the National Institute of Standards and Technology (NIST). The Lab includes a facility, testers, software, operating systems, network, and overall test strategies. All of these, working within government policies, guidelines and procedures form the basis of the Lab concept of operations.

In addition to testing products, the Lab provides consultation as well as research and development services to other federal agencies. This document only covers concepts involved with product Interoperability testing.



1.4 Background, Objectives, and Scope

The E-Authentication Initiative, part of the President's Management Agenda, will ultimately enable trust and confidence in E-Government transactions. Among other high-level objectives, the project will allow citizens and businesses simpler access to multiple applications via Single Sign-on capability and build an infrastructure and policy foundation for common authentication services.

Critical to the success of the E-Authentication Initiative is its ability to establish interoperable components from differing authentication technology. This challenge is addressed by the Lab, where Commercial off the Shelf (COTS) products, schemes and standards are evaluated and validated to determine their interoperability and appropriateness for the initiative.

The Lab provides an environment whereby General Services Administration (GSA) collaborates with other federal agencies and vendor representatives to establish base-line configurations of various COTS products to validate interoperability.

The Lab is not an information system. The Lab does *not* maintain production systems, or process transactions. It is established only as a test bed to prove product interoperability prior to deployment.

Interoperability in context of E-Authentication is enabling different Agency Applications (AA) to work together and exchange data with Credential Services Providers (CSP). Achievement of interoperability is through adherence to common standards and specifications.

The Lab does not validate products' conformance to standards, but does validate conformance to an E-Authentication Interface Specifications, which are subsets of industry standards.

The *E-Authentication Adopted Scheme Interface Specifications* provide the specifications against which products are tested to ensure interoperability with products on The Approved E-Authentication Technology Provider List.

1.5 Document Organization

The layout of this ConOps is largely based on the IEEE Std 1362-1998 and describes a situation and not a system. *Nothing in this document is confidential or business proprietary.* The remaining document is organized in the following sections:

- Section 2 - contains the technical and operational constraints and assumptions under which the Lab operates.
- Section 3 - provides a description and key characteristics of the Lab and an overview of its operating environment.
- Section 4 - describes the roles and responsibilities for the staff and organizations involved in the testing.
- Section 5 - describes operational processes that illustrate the role of the Lab, its interactions with users including vendors and agencies.
- Section 6 – describes the principles and practices that guide the Lab operation.

2 Constraints

The Lab's interoperability test criteria are constrained by:

- Applicable government standards, guidance and policies;
- The adoption of industry standards and schemes appropriate for the federated environment;
- The use of COTS products;
- Compliance with scheme matrix.

2.1 Applicable Government Policies, Guidance, and Standards

The Lab's test criteria are subject to standards, policies and guidance that are part of a larger policy framework including:

- Office of Management and Budget E-Authentication Guidance for Federal Agencies Memorandum (OMB M-04-04);
- National Institute for Standards and Technology Recommendation for Electronic Authentication (NIST SP 800-63);
- Federal PKI Bridge Certificate Policy (CP);
- GSA Information Technology (IT) Security Policy;
- Credential Assessment Framework;
- Federal Identity Credentialing Component.

2.2 Industry Standards and Interface Specifications

Industry standard specifications for technical schemes are used as the basis for interoperability testing. Use of these standards supports GSA's commitment to standards-based authentication solutions to U.S. government agencies. E-Authentication Initiative relies on these industry standards to create Interface Specifications. The Lab tests products for conformance to the initiative's own interface specifications, which are typical subsets of an industry standards, and interoperability with other certified products.

As new types and versions of schemes such as Security Assertion Markup Language (SAML) are released, the need for additional testing grows to ensure interoperability and conformance with them. It is an on-going challenge for the Lab and industry to ensure that as new protocols are developed and schemes adopted, a standards-based, interoperable, federated environment emerges.

The Lab verifies conformance with schemes such as SAML, an Organization for the Advancement of Structured Information Standards (OASIS), standard for the exchange of authentication and authorization information. In the future, E-Authentication may test products that are interoperable using Liberty Alliance, Shibboleth and WS-Federation.

2.3 Commercial off the Shelf (COTS) Products

The Lab focuses on COTS products for testing and certification. To be eligible, products must be available to federal buyers for purchase as a discrete product, preferably through an established federal contract such as the GSA Federal Supply Schedule.

The Lab tests beta versions of products to assist vendors in developing compliant products. However, this type of testing is a much lower priority than released software.

Open Source software is eligible for testing, but it must be sponsored by a federal or commercial organization.

2.4 Compliance with the Scheme Matrix

Products must not only conform to standards, but also be interoperable with other products. The following matrix must be completed for each product tested, as shown in Table 1. The matrix illustrates how products must interoperate with each other. This sample matrix records the product testing status and its ability to interoperate with other certified products.

Table 1: The Lab Scheme Status Matrix

		Credential services						
		A	**B**	**C**	**D**	E	F	G
Agency Applications	**A**		√	√	√	**O**	**-**	**-**
	B	√		√	√	**O**	**-**	**-**
	C	√	√		√	**-**	**-**	**-**
	D	√	√	√		**-**	**-**	**-**
	E	**O**	**O**	**-**	**-**		**-**	**-**
	F	**-**	**-**	**-**	**-**	**-**		**-**
	G	**X**	**X**	**X**	**X**	**X**	**X**	
	Test AA	√	√	√	√	√	**-**	**-**

Matrix Key:
√ Vendors are Interoperable
X Do Not interoperate
O Currently testing and trouble shooting
- Testing not attempted

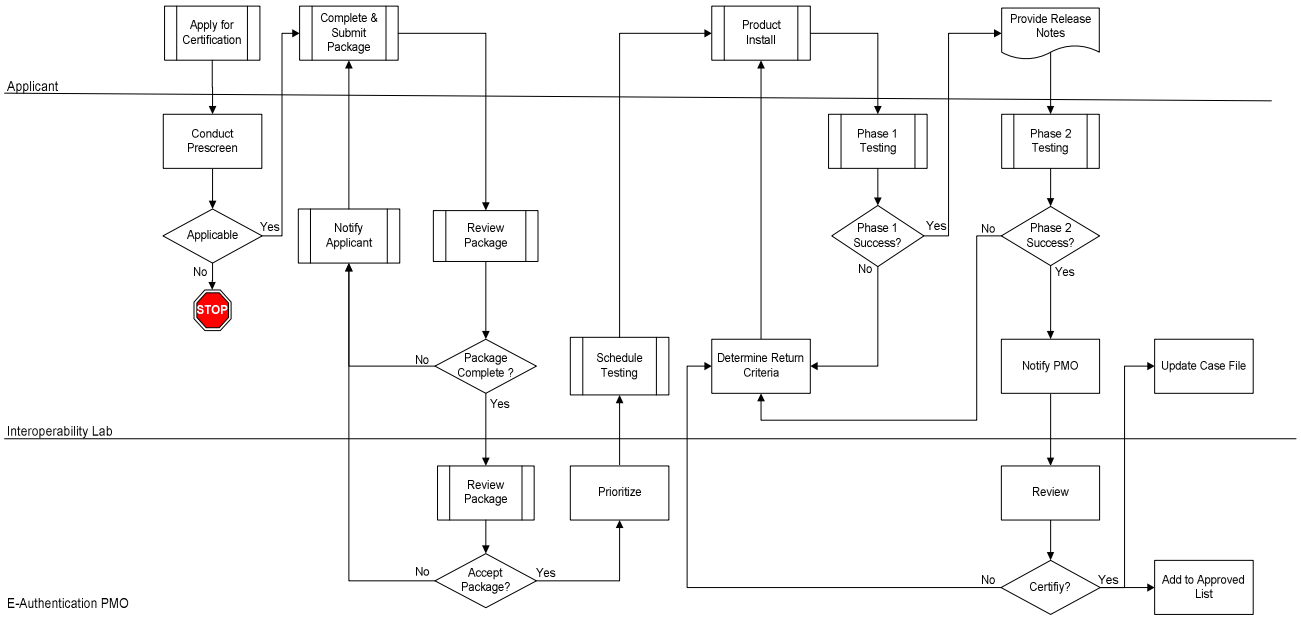
3 Concept Description and Scenarios

3.1 Concept Overview

Figure 1 depicts the overall Lab's concept of operations.

At the highest level, Applicants, Agencies, and CSPs apply for certification; the Lab reviews the application and determines if testing is merited. If so, the Applicant provides an appropriately licensed product, which is installed, configured and tested by Lab personnel. If the product is deemed conformant to the Interface Specification and is interoperable, then the product is recommended for certification to the PMO. The three main user groups are the Applicant, Lab, and the E-Authentication Program Management Office (PMO).

Figure 1: Interoperability Lab Concept of Operations Process



The Lab concept is based on a collection of:

- Services and Functions;
- Personnel, Staff and Organization;
- Process and Activities;
- Overarching Guiding Principles and Practices.

3.2 Services and Functions

There are a number of sub-functions that support interoperability testing, such as testing schemes, product verification, and hosting special testing events. The primary service offerings of the Lab are outlined below:

Table 2: Services and Functions

Services and Functions	Function Description
Test Candidate Schemes	When three or more COTS products that purport to comply with a scheme or standard, the Lab tests the products for interoperability and considers the new scheme for adoption.
Conformance Verification	Analyze and verify product compliance and conformance with scheme specifications.
Interoperability Certification	A product is considered "interoperable" when it successfully demonstrates interoperability as an AA and a CS, with all approved products on the Approved E-Authentication Technology Provider list.
Host Special Test Event	Agency Specific Test - test products for interoperability in pre-specified operating environments that conform to the unique hardware and software platforms of an agency. Industry Days - days open to agencies and vendors who want to participate in informal interoperability testing in a collaborative environment to determine how well their respective products interoperate. This does not result in certification but allows vendors and agencies to work together on new product offerings prior to requesting formal certification testing.
Resolve interoperability Issues	If a product on the Approved E-Authentication Technology Provider List is found to be non-conformant with the Interface Specifications (not interoperable), the Lab will assist in resolving the issue, retest the product and forward the matter to the PMO if necessary. The Lab will document the outcome or recommendations to avoid future reoccurrences of the problem.
Publication	After the E-Authentication PMO certifies the product, the PMO publishes the Approved E-Authentication Technology Provider List, Interoperability Requirements, Technical Specifications, Guidance and Schemes.

4 Roles and Responsibilities

Within the Lab, there are roles and responsibilities that are carried out by Lab personnel and other organizations. These roles and responsibilities are described below.

4.1 Applicant

An Applicant is an individual or organization who requests interoperability certification for a product as an AA and CS. The relationship of the Applicant to the AA or CS may vary. In most cases, the Applicant will be the actual developer of the AA or CSP COTS product. However, this may not always be the case. The Applicant may be an agency, an organization, or an individual involved in the acquisition of an IT system that includes that particular product as a key component. The Applicant may be an independent contractor, serving as a systems developer or integrator attempting to fulfil the requirements of a contract. Other situations may apply.

In cases where the Applicant is not the developer of the product, the Applicant needs to obtain the cooperation of the developer in providing the Lab with technical materials and essential deliverables necessary to conduct the evaluation in a complete and consistent manner. The specific details of the provision of documentation for the evaluation will be handled in contractual agreements between the applicant and the agency or CSP.

4.2 Lab Manager

The Lab Manager is responsible for the overall operation of the Lab including oversight of testing and quality assurance. The Lab Manager is responsible for:

- Sets the strategies and goals for the Lab;
- Assigning resources for testing;
- Ensuring all Lab operations adhere to the security and confidentiality requirements;
- Makes efficient, effective use of the Lab's staff and other resources;
- Performing all test activities are performed consistent with the ConOps and Lap Operations Manual;
- Briefs management and Applicants on testing status;
- Review and resolve all dispute/complaint submissions, escalating to the PMO where appropriate.

4.3 Technical Evaluation Team / Lab Engineers

The technical evaluation team is comprised of system engineers, test specialists, lab coordinator, system administrators, lead technician and network administrators. This team is the single point of contact for Applicant interaction and testing. The team is specifically responsible for:

- The coordination of applicants applying for certification;
- Managing internal network and systems;

- Preparing the environment for testing—including establishing baselines for systems and the network environment;
- Installing, configuring, troubleshooting, and testing products;
- Concluding whether products meet E-Authentication Interface Specification requirements;
- Providing technical expertise to Applicants and certified product vendors.

4.4 Certified Product Vendors

Certified product vendors are those that have products successfully tested by the Lab with demonstrated interoperability. These vendors are responsible for maintaining their products in a state that is interoperable and for preparing adequate reference materials for agencies to install and configure their products properly.

4.5 E-Authentication Program Management Office (PMO)

The E-Authentication PMO is responsible for; overseeing all test activities of the Lab, to ensure consistent and unbiased testing; for maintaining and approving updates to the Lab policies and procedures.

The PMO will ensure that appropriate mechanisms are in place to protect the interests of all parties, and is responsible for resolving any disputes concerning the operation of the Lab or any of its associated activities

The PMO is responsible for final notification to Applicants. PMO does not release Applicant information to the public until they are on the Approved E-Authentication Technology Provider List.

5 Process Descriptions

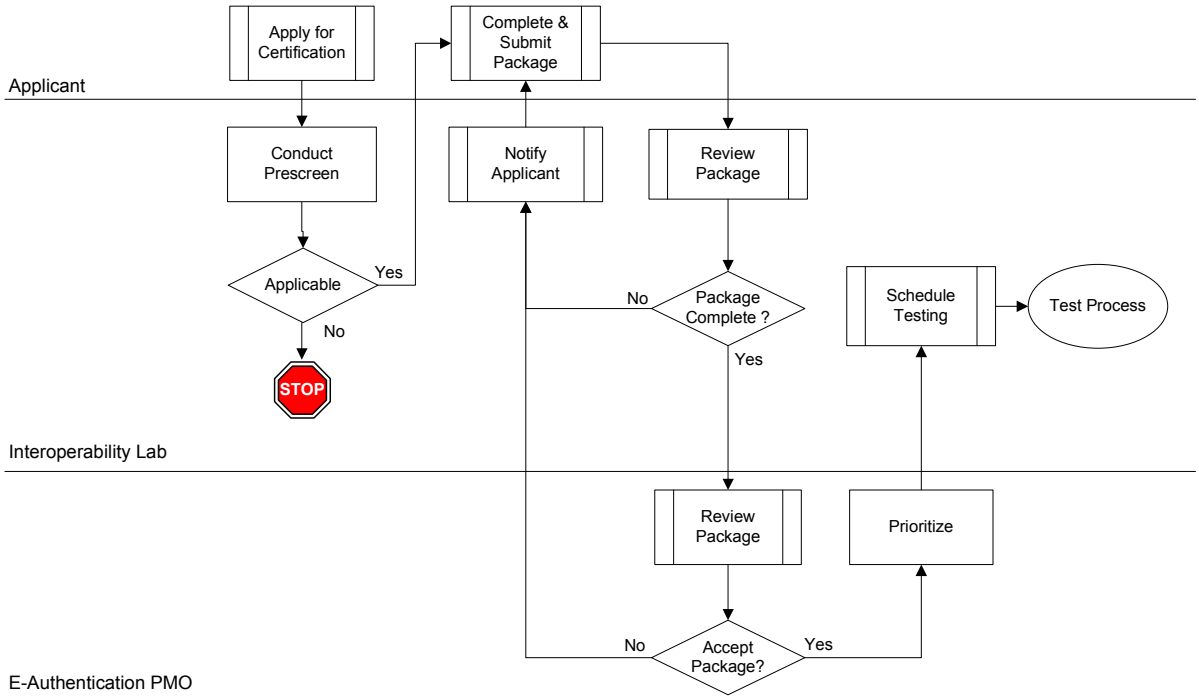
The following sections describe the steps for obtaining Interoperability certification as illustrated in Figure 5-1. The three (3) primary processes are:

1. Application Process;
2. Testing and Certification Process;
3. Maintenance Process.

5.1 Application Process

The process for receiving, vetting and accepting applications is depicted in Figure 2 below.

Figure 2: Application Process



5.1.1 Apply for Certification

The first step is pre-screening to determine if the product's capabilities are aligned with the E-Authentication Initiative and should be tested for interoperability. This is typically a teleconference conducted before the applicant invests time completing the Application Package. Products not suited for interoperability testing as an AA or CS, but of potential importance to the E-Authentication Initiative, may be evaluated for compatibility with the E-Authentication technical architecture as part of the Lab's R&D program.

The Applicant may request pre-screening by submitting an email to interoplab@enspier.com. GSA may announce the opening of testing through one of several means including a Request For Information (RFI), Federal Register Announcement, or through the E-Authentication web site.

5.1.2 Complete and Submit Application Package

If the product is determined to be appropriate, then the next step for the Applicant is to complete the Application Package. The Application Package is available from the E-Authentication Initiative's website. Applicants must complete the Application Package and submit it for review to be considered for testing. The Application Package contains the following:

1. Product Questionnaire;
2. Scheme Assessment Form;
3. Non-Disclosure Agreement;
4. License Agreement.

5.1.3 Review Package and Notify Applicant

Acceptance or denial of each package will be decided upon using the following evaluation criteria:

- Applicant has successfully completed the product questionnaire (all required information is provided and complete).
- Applicant has completed the scheme assessment form.
- Product is a commercially released version.
- Product is an appropriate fit for the E-Authentication Initiative.
- Product purports compliance with one or more of the adopted schemes.

Upon receipt of the package, the Lab will review it to determine if it is complete. If incomplete, the applicant will be provided with an Application Findings Letter stating what the findings were and information on next steps for the Applicant.

The Lab will retain a copy of the Application Package. An incomplete Application Package will be held on file for 30 days, and destroyed after 90 days if deficiencies are not addressed.

If complete, the Application Package is sent to the PMO for acceptance and a priority assignment. If accepted, the Applicant is invited to participate in Phase 1 - Interoperability Analysis.

5.1.4 Schedule Testing

The accepted applications will be forwarded to the Lab Manager from PMO. The Lab Manager will assign resources and determine the test schedule based on the priority assigned by the PMO. The Lab Manager will identify project constraints specifying time, equipment, funding, and personnel. The Lab Manager will form the Technical Evaluation Team and appoint a team lead. The team lead will coordinate with the Lab Manager, Technical Evaluation Team, Applicant, and the Applicant's Technical Representatives. The team lead will serve as the single point of contact for the applicant and the applicant's technical representatives.

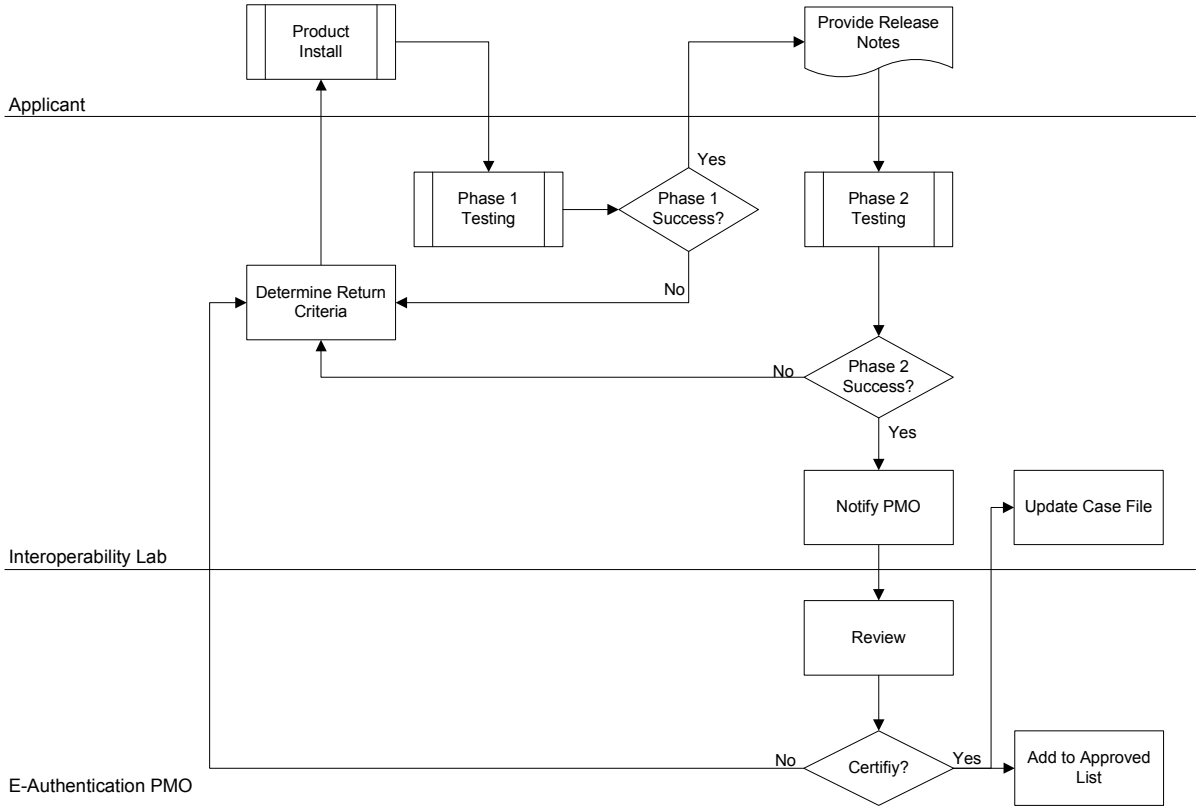
The Technical Evaluation Team will ensure the scope of testing is determined and the requirements are well defined and testable.

The Technical Evaluation Team lead will schedule the applicant for testing based on the earliest slot available for the adopted scheme used by the product. The Applicant's Technical Representative must provide a copy of the software for installation.

5.2 Test Process

The Lab uses a phased approach to testing, which is depicted in Figure 3 below.

Figure 3: Testing & Certification Process



5.2.1 Product Installation

Applicants are given access to a room at the Lab to configure equipment and install their product. A Lab Engineer will be available to answer questions and aid in troubleshooting.

The Applicant must set up the product for configuration as both a CS and an AA. Lab Engineerss must be shown how to configure the product as CSs and AAs. Before any testing begins, the product is configured to interoperate with three other products. Successful interaction with the three vendors does not constitute success.

While it is important to the PMO that Applicants be provided as much of an open environment as possible, it is as equally important to maintain anonymity. Whenever technicians are experiencing difficulty with a product, the Applicant is contacted as soon as possible to resolve the issue. If the Technical Evaluation Team determines that the issue may involve the certified product, the team contacts the vendor of that product as well.

5.2.2 Phase 1 – Interoperability Analysis

Phase 1 - Interoperability Analysis, a trial and discovery round, conducted with the Applicant's technical representatives present. These representatives work with the Technical Evaluation Team to ensure that the product is installed properly in the Lab and that all configuration issues are resolved. If the applicant's technical representatives are unable to resolve installation or configuration issues to the satisfaction of the Technical Evaluation Team, or if the appropriately licensed product requires modification, the process will be suspended. The Lab will notify the Applicant and provide them with a detailed log identifying each issue. Applicants may request lab time for testing to ensure that product changes to support interoperability are effective before re-releasing a new version of the product

When all issues are resolved the product is retested. When Phase 1 is successful, the applicant is invited to participate in the Phase 2 - Certification Test. The applicant must submit updated Installation and Administration Documentation for their product to be accepted for Phase 2 Certification Test.

5.2.3 Phase 2 – Certification Test

Phase 2 testing is performed on a clean test environment by only the Technical Evaluation Team. The Applicant can not directly interact with the product, the Technical Evaluation Team will execute the tests, collect, and examine all available test data.

All Phase 2 issues are recorded and maintained by the Lab. The Lab will notify the Applicant when issues arise providing them with a detailed log identifying each issue. When products have successfully completed Phase 2 testing, the Lab will request a letter from the vendor verifying the product's name and version number as well as service packs and patches. When this is received, the Lab will send the Interoperability Test Summary to the Lab Manager to notify the PMO for official product certification.

5.2.4 E-Authentication Program Management Office Notification

The PMO makes the final certification decision, assigning:

Interoperable - Product meets all certified interoperability requirements and is added to the Approved E-Authentication Technology Provider List.

Not Interoperable - Product does not meet interoperability standards and is not recommended for the Approved E-Authentication Technology Provider List.

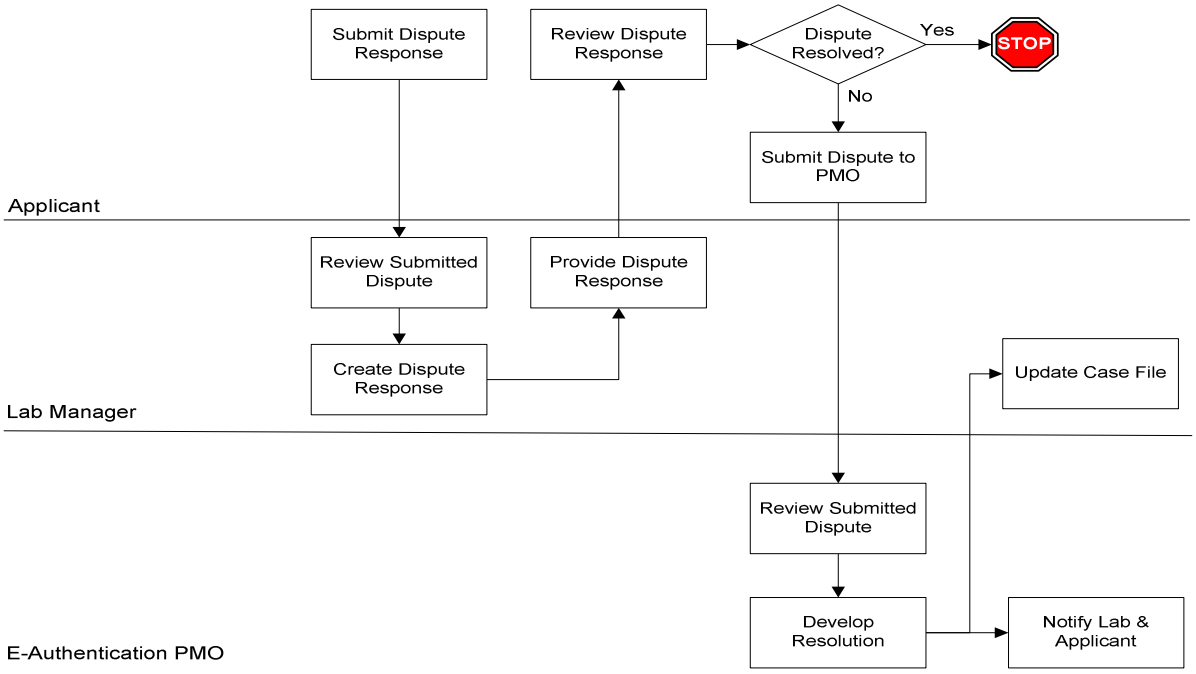
Once the product has been officially determined Interoperable, the Lab will send the Phase 2 Certification Letter to the Applicant notifying them that the product has achieved Full Interoperability Certification and will be added to The Approved E-Authentication Technology Provider List.

During Interoperability testing of a new product, a product that has already been certified to be Interoperable may be found later to be not-compliant with Interface Specifications. If this occurs, the Certified Product Vendor will be notified of the issue and is given 15 business days to take corrective action. The PMO has the authority to remove any product from the Approved E-Authentication Technology Provider List.

5.3 Dispute Resolution Process

The process of resolving disputes that arise between Applicants and the Lab is depicted in Figure 4.

Figure 4: Dispute Resolution Process



An Applicant that has a dispute with a Lab decision must submit a Dispute Resolution Form to the Lab Manager. The form may be submitted electronically to the Lab. The form is reviewed for completeness. Incomplete submissions are returned to the Applicant, who has 15 days to re-submit their disputes.

The Lab Manager reviews the submission and researches the facts of the dispute. This review includes thoroughly examining all documentation in the case file and interviewing the Technical Evaluation Team assigned to the Applicant.

The Lab Manager then discusses the submission and findings with the Applicant. If the dispute is resolved during this discussion, the Lab Manager documents that result. The Lab then issues a formal letter of the resolution to the Applicant and places a copy in the case file. If the dispute cannot be resolved in that discussion to the satisfaction of both parties, the situation is escalated to the PMO. The original dispute submission, the results of the research performed by the Lab Manager and the entire contents of the case file are made available to the PMO, if necessary.

The PMO determines a solution to the dispute and prepares a report that outlines the solution and explains what led them to that decision. The PMO then notifies the Applicant and the Lab of its decision and the case file is updated.

In some cases, the evaluation performed and the resolution developed by the PMO could result in modifications to the Lab's policies and procedures.

Some examples of disputes that could arise include:

1. Applicant believes its Application Package was wrongfully denied by the Lab.
2. Applicant disagrees with the testing procedures used for testing its product.
3. Applicant believes its product was not tested in a fair and ethical manner.
4. Applicant disagrees with the testing results.
5. Applicant disagrees with certification determination (situations in which the Lab tested the product as fully interoperable, but the PMO decided not to add the product to the certification list).
6. Applicant believes it should have more time, beyond the 15 days set forth by the Lab policies, to fix problems with its product.

6 Guidance Principles and Practices

6.1 Privacy and Confidentiality

Some of the information collected and maintained by the Lab is proprietary to participating vendors. This proprietary information could include something as simple as the desire to test in the Lab, Lab results, or possibly engineering information about a product. For this reason, all Lab personnel including vendors must sign agreements to prevent the disclosure of proprietary information.

6.2 Scheduling

The Lab operates on a block schedule approach that allows the Lab to focus on a particular scheme or set of related products. For example, April 1-20 might be dedicated to SAML, while May 1-20 may be dedicated to Liberty products. Accordingly, the Lab could be closed during a block of time for maintenance or to prepare for a new scheme.

6.3 Security

The need for security in the Lab is critically important, especially when considering the risk of disclosing proprietary information. To ensure adequate security controls are in place, the Lab institutes appropriate management controls, operational controls and rules of conduct.