E-Authentication Interoperability Lab Concept of Operations

Version 2.0.0
June 06, 2005

Executive Summary

The document describes the operation concepts of the E-Authentication Interoperability Lab (Lab). The Lab tests software products, services, and Authentication Service Component (ASC) components for compliance to E-Authentication's Interface Specifications, which are a subset of industry standards. In addition, the Lab tests software products for interoperability with the approved software products that purport the same compliance.

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 testing of software products, services, and Authentication Service Component (ASC) components, as well as unbiased test results. The basic premise of this concept of operations 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.

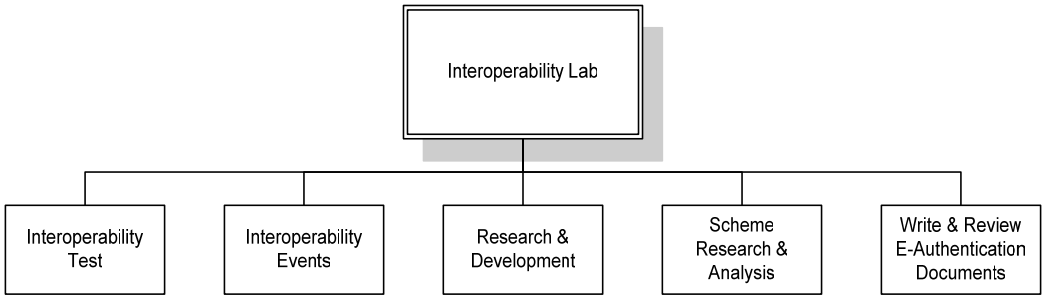
1.3 E-Authentication Interoperability Lab

The core function of the Lab is to analyze, test and certify the interoperability of software, services, and ASC components that desire interoperability testing. The Lab is a unit of the E-Authentication Initiative (Initiative) and is sponsored by the General Service Administration (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 software product, services, and ASC component testing, the Lab provides the following services:

- Research and development services to other Federal Agencies;
- Hosts interoperability events;
- Research and analysis of new schemes;
- Write and review E-Authentication documents.

Figure 1: Interoperability Lab Services



While the Lab provides several services for the Initiative, this document only covers concepts involved with software product, services, and ASC component testing.

1.4 Services and Functions

As mentioned, there are a number of sub-functions that support Lab operations. The primary service offerings of the Lab are outlined below:

Table 1: Services and Functions

Services and Functions	Function Description
Test Candidate Schemes	When there are three or more software products that purport to comply with a scheme or standard, the Lab tests the software products for interoperability and considers the new scheme for adoption.
Compliance Verification	Analyze and verify software products, services, and ASC component compliance with scheme specifications.
Interoperability Certification	A software product, service, or ASC component is considered "interoperable" when it successfully demonstrates interoperability with all currently approved software products on *The Approved E-Authentication Technology Provider list.*
Host Special Test Event	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 approval but allows vendors and Agencies to work together on new product offerings prior to requesting formal approval testing.
Resolve Interoperability Issues	If a software product on *The Approved E-Authentication Technology Provider List* is found to be non-compliant with the *E-Authentication Interface Specifications*, the Lab will assist in resolving the issue, retest the software product and forward the matter to the Program Executive if necessary. The Lab will document the outcome or recommendations to avoid future reoccurrences of the problem.
Write & Review E-Authentication Documents	The Lab is responsible for the developing technical documentation (e.g., software product configuration guides, Agency Application (AA) and Credential Service (CS) test suites) as it is needed by the Initiative. Additionally, the Lab is responsible for reviewing and commenting on other Initiative documentation (e.g., Interface Specifications, Architecture Change Proposals).

1.5 Background, Objectives, and Scope

The 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 online government applications via single sign-on (SSO) capability and build an infrastructure and policy foundation for common authentication services.

Critical to the success of the Initiative is its ability to establish interoperable components from differing authentication technology. This challenge is addressed by the Lab, where software products, services, ASC components, schemes and standards are evaluated and validated to determine their interoperability and appropriateness for the Initiative.

The Lab provides an environment whereby GSA collaborates with other Federal Agencies, Credential Service Providers (CSPs), and vendor representatives to validate interoperability. The Lab is not considered an information system and does *not* maintain production systems, or process transactions. It is established only as a test bed to prove interoperability prior to deployment.

Interoperability in context of E-Authentication is enabling different AAs to work together and exchange data with CSs. Achievement of interoperability is through adherence to common standards and specifications.

The Lab does not validate software product, service, or ASC component compliance to standards, but does validate compliance to the *E-Authentication Interface Specifications*, which are subsets of industry standards. The *E-Authentication Adopted Scheme Interface Specifications* provide the specifications against which software products, services, and ASC components are tested to ensure technical interoperability with software products on *The Approved E-Authentication Technology Provider List*.

1.6 Document Organization

The layout of this ConOps is largely based on the IEEE Std 1362-1998 and describes a support process 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 – describes the roles and responsibilities for the staff and organizations involved in testing.
- Section 4 – describes operational processes that illustrate the role of the Lab and its interactions with software products.
- Section 5 – describes operational processes that illustrate the role of the Lab and its interactions with services.
- Section 6 – describes operational processes that illustrate the role of the Lab and its interactions with ASC components.
- Section 7 – describes the dispute resolution process and illustrates the role of the Applicant, Lab Manager, and Operations Director.
- Section 8 – describes the principles and practices that guide the Lab operation.

2 Constraints

The Lab's interoperability test criteria are constrained by the following:

- Applicable government standards, guidance and policies;
- The adoption of industry standards and schemes appropriate for the federated environment;
- The use of software products;
- The use of services;
- The use of ASC components;
- 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 but no limited to:

- 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;
- Homeland Security Presidential Directive (HSPD) – 12.

2.2 Industry Standards and Interface Specifications

Industry standard specifications for technical schemes are used by the Lab as the basis for interoperability testing. Use of these standards supports GSA's commitment to standards-based authentication solutions to U.S. government Agencies. The Initiative relies on these industry standards to create Interface Specifications. The Lab tests software products, services, and ASC components for compliance to the *E-Authentication Interface Specifications* and tests for interoperability with approved software products.

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

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

2.3 Software Products

One function of the Lab is to conduct software product testing, which includes the testing of the following:

- Commercial off the Shelf (COTS) products;

- Toolkits;
- Open source software.

To be eligible, COTS products and toolkits must be available to the Federal government for purchase as a discrete product, preferably through an established Federal contract such as the GSA Federal Supply Schedule. Open source software products are eligible for testing, but must be sponsored by a Federal Agency. Additionally, all software products cryptographic operations must be in compliance with approved cryptographic techniques (FIPS approved and/or NIST recommended), and implemented in at least a FIPS 140-2 Level 1 cryptographic module to be eligible for testing in the Lab.

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

2.4 Services

Another function of the Lab is to conduct service testing, which includes the testing of AAs and CSs. To be eligible for testing, an AA or CS must be configured with one of the approved software products.

2.5 ASC Components

The other function of the Lab is to conduct ASC component testing, which includes the testing of the following:

- Scheme Translators;
- Step Down Translators (SDTs);
- E-Authentication Portal (Portal).

To be eligible for testing, the ASC component must be approved for testing by the Operations Director.

2.6 Compliance with the Scheme Matrix

Software products must not only conform to standards, but also be interoperable with the approved software products. The following matrix must be completed for each software product tested, as shown in Table 2. The matrix illustrates how software products must interoperate with each other. This sample matrix records the software product testing status and its ability to interoperate with approved software products.

Table 2: 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 Roles & 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.

3.1 Applicant

There are several types of applicants that may request testing in the Lab. An Applicant consists of one of the following:

- Individual or organization who requests interoperability certification for a software product as an AA and/or CS. The relationship of the Applicant to the AA or CS may vary. In some cases, the Applicant can be the actual developer of the software product. However, this may not always be the case.
- Agency, CSP, an organization, or an individual involved in the acquisition of an IT system that includes that particular product as a key participant.
- An owner or person responsible for an ASC component.
- An independent contractor, serving as a systems developer or integrator attempting to fulfil the requirements of an Agency contract. Other situations may apply.

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

3.2 Lab Manager

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

- Setting the daily goals for the Lab;
- Assigning resources for testing;
- Ensuring all Lab operations adhere to the security and confidentiality requirements;
- Making efficient, effective use of the Lab's staff and other resources;
- Ensuring all test activities are performed consistent with the ConOps and Lab Operations Manual;
- Briefing management and Applicants on testing status;
- Maintaining updates to the Lab policies and procedures.

3.3 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:

- Assisting applicants with the application process;
- Managing internal network and systems;
- Preparing the environment for testing—including establishing baselines for systems and the network environment;

- Installing, configuring, troubleshooting, and testing software products, services, and ASC components;
- Concluding whether software products, services, and ASC components meet *E-Authentication Interface Specification* requirements;
- Providing technical expertise to Applicants and approved software product vendors.

3.4 Approved Software Product Vendors

Approved software product vendors are those who are responsible for software products that have demonstrated interoperability and are approved for E-Authentication participation. These vendors are responsible for maintaining their software product in compliance with the *E-Authentication Interface Specifications* and for preparing adequate reference materials for Agencies and CSPs to install and configure their software product properly.

3.5 Approved Service Owners

Approved service owners are Agencies and CSPs who's AAs and CSs have demonstrated interoperability and are approved for E-Authentication participation. Agencies and CSPs who own an approved AA or CS are responsible for maintaining the AA or CS in a state that is interoperable.

3.6 Approved ASC Component Owners

Approved ASC component owners are those who are responsible for ASC components that have demonstrated interoperability and are approved for E-Authentication participation. ASC component owners are responsible for maintaining the ASC component in a state that is interoperable.

3.7 Relationship Managers

For the testing of services, the Agency and CSP Relationship Managers have the following responsibilities:

- Requesting Lab time for testing an AA or CS;
- Providing Agencies or CSPs on testing status;
- Answering any questions an Agency or CSP has in regard to service testing.

3.8 Operations Manager

In regard to Lab operations, the Operations Manager has the following responsibilities:

- Reviewing and approving application packages;
- Prioritizing testing;
- Reviewing and resolving all dispute/complaint submissions, escalating to the Operations Director where appropriate;
- Providing Agencies or CSPs with a waiver that allows the use of an unapproved software product.

3.9 Operations Director

In regard to Lab operations, the Operations Director is responsible for the following:

- Requesting Lab time for testing ASC components;
- Providing final software product approval;
- Providing final services approval;

- Providing final ASC component approval;
- Adding all approved software products, services, and ASC components to their appropriate approved list;
- Resolving any unresolved disputes concerning the operation of the Lab or any of its associated activities.

3.10 Program Executive

In regard to Lab operations, the Program Executive has the following responsibilities:

- Overseeing all test activities of the Lab;
- Ensure consistent and unbiased testing;
- Approving updates to the Lab policies and procedures;
- Ensure that appropriate mechanisms are in place to protect the interests of all parties.

For software product, service, and ASC component testing, the Initiative does not release Applicant information to the public until being placed on their appropriate approved list.

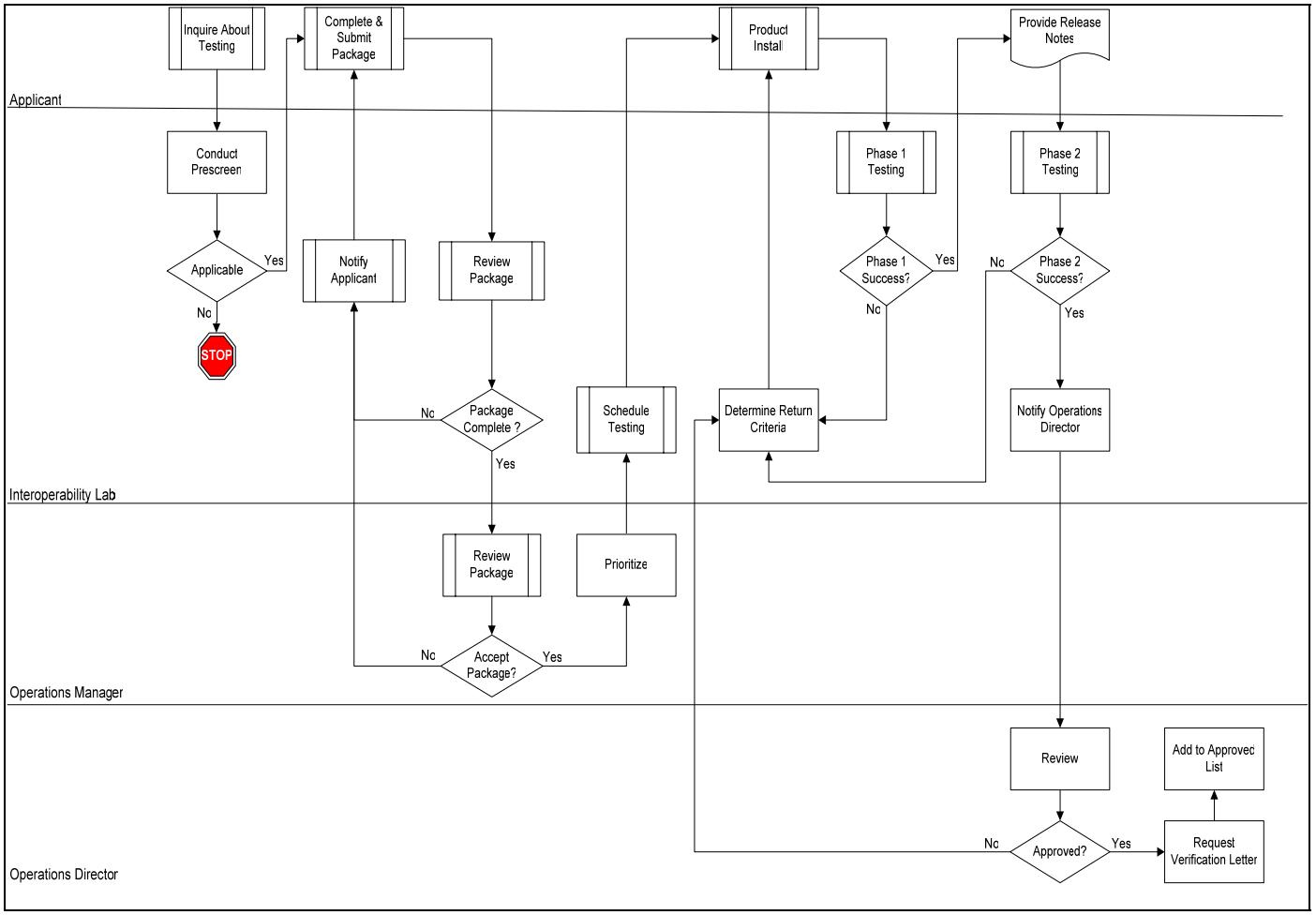
4 Software Product Testing

4.1 Concept Overview

Figure 2 depicts the Lab's overall concept of operations for testing software products.

At the highest level, software product vendors or representatives apply for certification; the Lab and Operations Manager review the application and determine if testing is in the best interest of the Federal government. If so, the Applicant provides an appropriately licensed software product, which is installed, configured and tested by the Technical Evaluation Team. If the software product is deemed compliant to the Interface Specification and is interoperable, then the software product is recommended for approval by the Operations Director. The four main user groups are the Applicant, Lab, Operations Manager, and Operations Director.

Figure 2: Interoperability Lab Concept of Operations Process for Software Product Testing



This Lab concept is based on a collection of:

- Personnel, Staff and Organization (Section 3);
- Process and Activities;
- Principles and Practices (Section 8).

4.2 Process Description

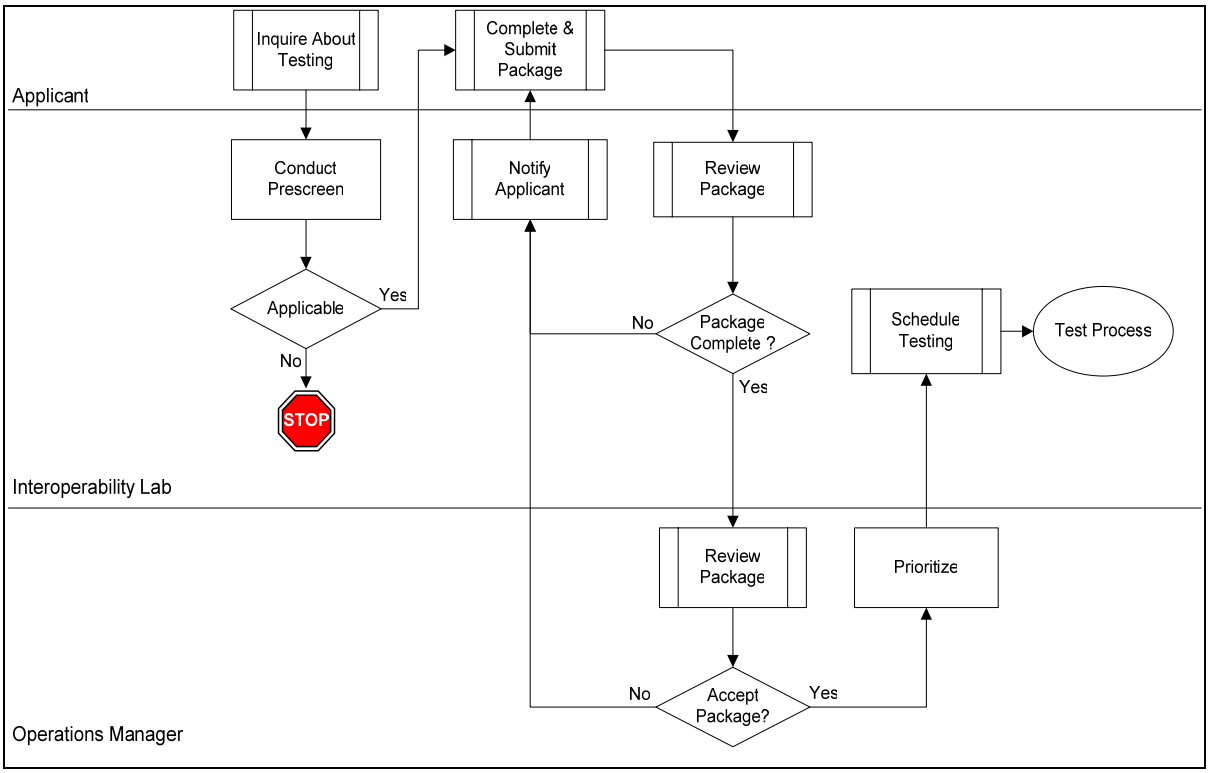
The following sections describe the steps for software products becoming approved technology providers. The two (2) primary processes are:

1. Application Process;
2. Testing and Approval Process.

4.2.1 Application Process

The process for receiving, vetting and accepting applications is depicted in Figure 3 below.

Figure 3: Application Process



4.2.1.1 Inquire About Testing

The first step is for the Applicant (software product vendor or representative) to contact the Lab for inquiring about software product testing. Next, the Lab pre-screens the Applicant to determine if their software product's capabilities are aligned with the Initiative and should be tested for interoperability. This is typically a teleconference conducted before the Applicant invests time completing the Application Package. Software products not suited for interoperability testing, but have potential importance to the Initiative, may be evaluated for compatibility with the E-Authentication technical architecture as part of the Lab's Research & Development program.

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

4.2.1.2 Complete and Submit Application Package

If the software product is determined to be in the best interest for the Federal government, then the next step is for the Applicant to complete the Application Package. The Application Package is available from the Initiative's web site (http://www.cio.gov/eauthentication). Applicants must complete the Application Package and submit it to interoplab@enspier.com for review and consideration for testing. The Application Package contains the following:

1. Product Questionnaire;
2. Scheme Assessment Form;
3. Lab Service Agreement.

4.2.1.3 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 and signed the Scheme Assessment Form;
- Applicant has completed and signed the Lab Service Agreement;
- Software product is a released version;
- Software product is FIPS approved or NIST recommended, and implemented in at least a FIPS 140-2 Level 1 cryptographic module;
- Software product is an appropriate fit for the Initiative and in the best interest of the Federal government;
- Software product purports compliance with one or more of the adopted schemes.

Upon receipt of the package, the Lab will review it for completeness. If incomplete, the Applicant will be notified and provided information on next steps.

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 Operations Manager for approval and priority assignment. If accepted, the Applicant is invited to participate in Phase 1 - Interoperability Analysis.

4.2.1.4 Schedule Testing

All accepted applications are forwarded from the Operations Manager to the Lab Manager. Upon receipt, the Lab Manager will assign resources and determine the test schedule based on the priority assigned by the Operations Manager. 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.

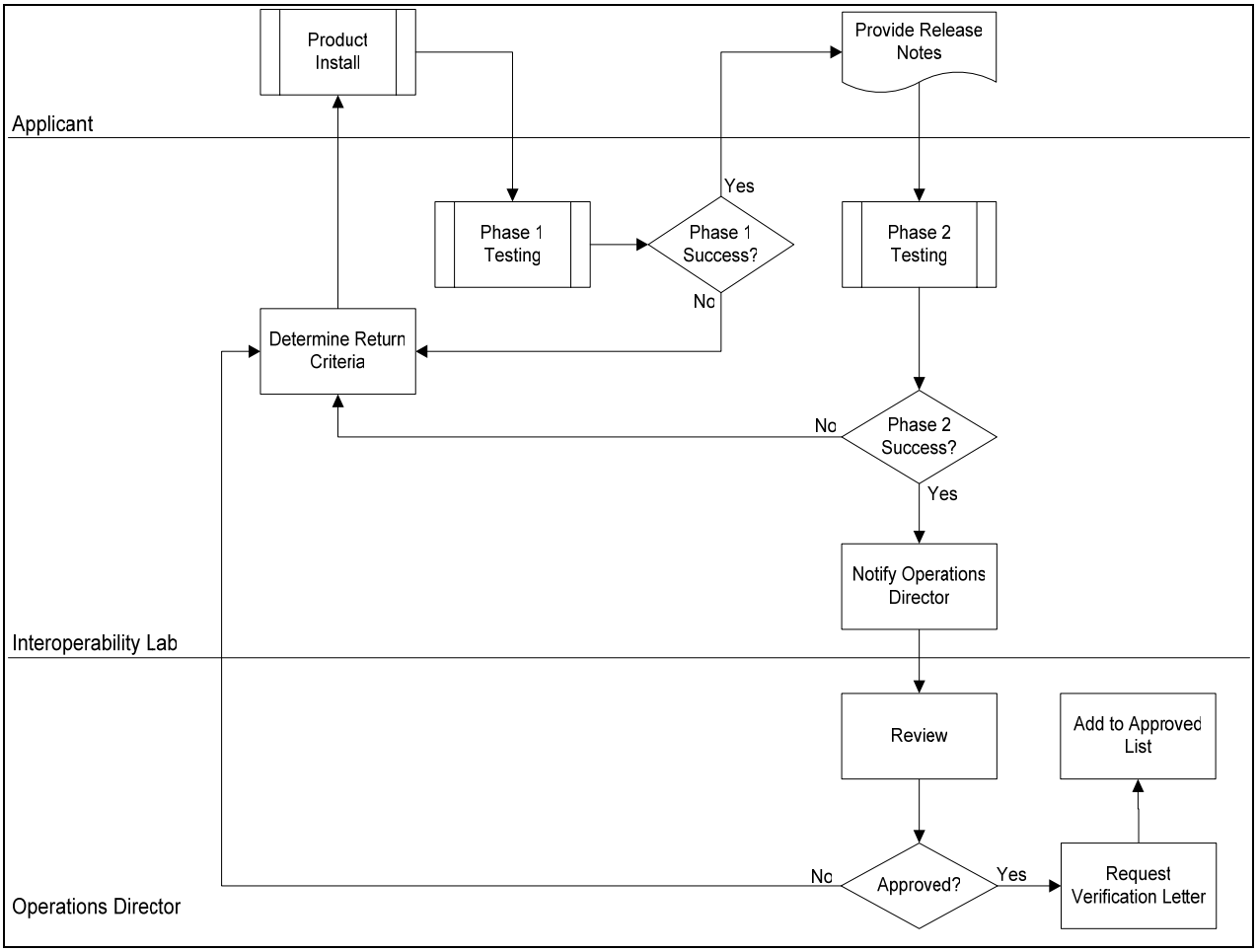
The Technical Evaluation Team will ensure the scope of testing is determined and the requirements are well defined and testable. If needed, the Technical Evaluation Team will hold a teleconference with the Applicant's Technical Representative to discuss any remaining issues.

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

4.2.2 Testing & Approval Process

The Lab uses a phased approach to testing, which is depicted in Figure 4 below.

Figure 4: Testing & Approval Process



4.2.2.1 Product Installation

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

The Applicant must set up the software product for configuration as both a CS and/or AA, and Lab Engineers must be shown how to configure the software product as a CS and/or AA. Before any testing begins, the software product is configured to interoperate with three (3) approved software products. Successful interaction with the three software products does not constitute success. An Applicant is limited to three (3) days for software product installation. If more time is needed, the Applicant will need to schedule for more time in the Lab to complete the installation.

While it is important that Applicants be provided as much of an open environment as possible, it is as equally important to maintain anonymity. Whenever the Technical Evaluation Team is experiencing difficulty with a software product, the Applicant is contacted as soon as possible to resolve the issue. If it is determined that the issue may involve an approved software product against which the Applicant's

software product is being tested, the Technical Evaluation Team will contact the vendor of the approved software product as well.

4.2.2.2 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 software 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 software product requires modification, the process will be suspended. The Technical Evaluation Team will notify the Applicant and provide the identified issues. Applicants may request Lab time for testing to ensure that software product changes to support interoperability are effective before releasing a new version of the software product.

The software product is retested when all issues are resolved. When Phase 1 is determined successful, the Applicant is notified and invited to participate in Phase 2 - Certification Test.

4.2.2.3 Phase 2 – Certification Test

Phase 2 testing is performed on a clean test environment (i.e., separate from Phase 1 testing environment) by only the Technical Evaluation Team. The Applicant is not permitted to interact with the software product; the Technical Evaluation Team will execute the tests, collect, and examine and report on all available test data.

All Phase 2 issues are recorded and maintained by the Lab. The Technical Evaluation Team will notify the Applicant when issues arise and provide the identified issues. When software products have successfully completed Phase 2 testing, the Lab Manager will notify the Operations Director for official software product approval.

4.2.2.4 Operations Director Notification

The Operation Director makes the final approval decision, assigning:

Interoperable – Software product meets all certified interoperability requirements and is added to *The Approved E-Authentication Technology Provider List.*

Not Interoperable – Software product does not meet interoperability standards and is not recommended for *The Approved E-Authentication Technology Provider List.*

Once the final approval decision has been made, the Operations Director will notify the Applicant and request that the Applicant provide a letter verifying the software product's name, version number, and service packs and patches. Once the letter has been received, the software product will be added to *The Approved E-Authentication Technology Provider List*.

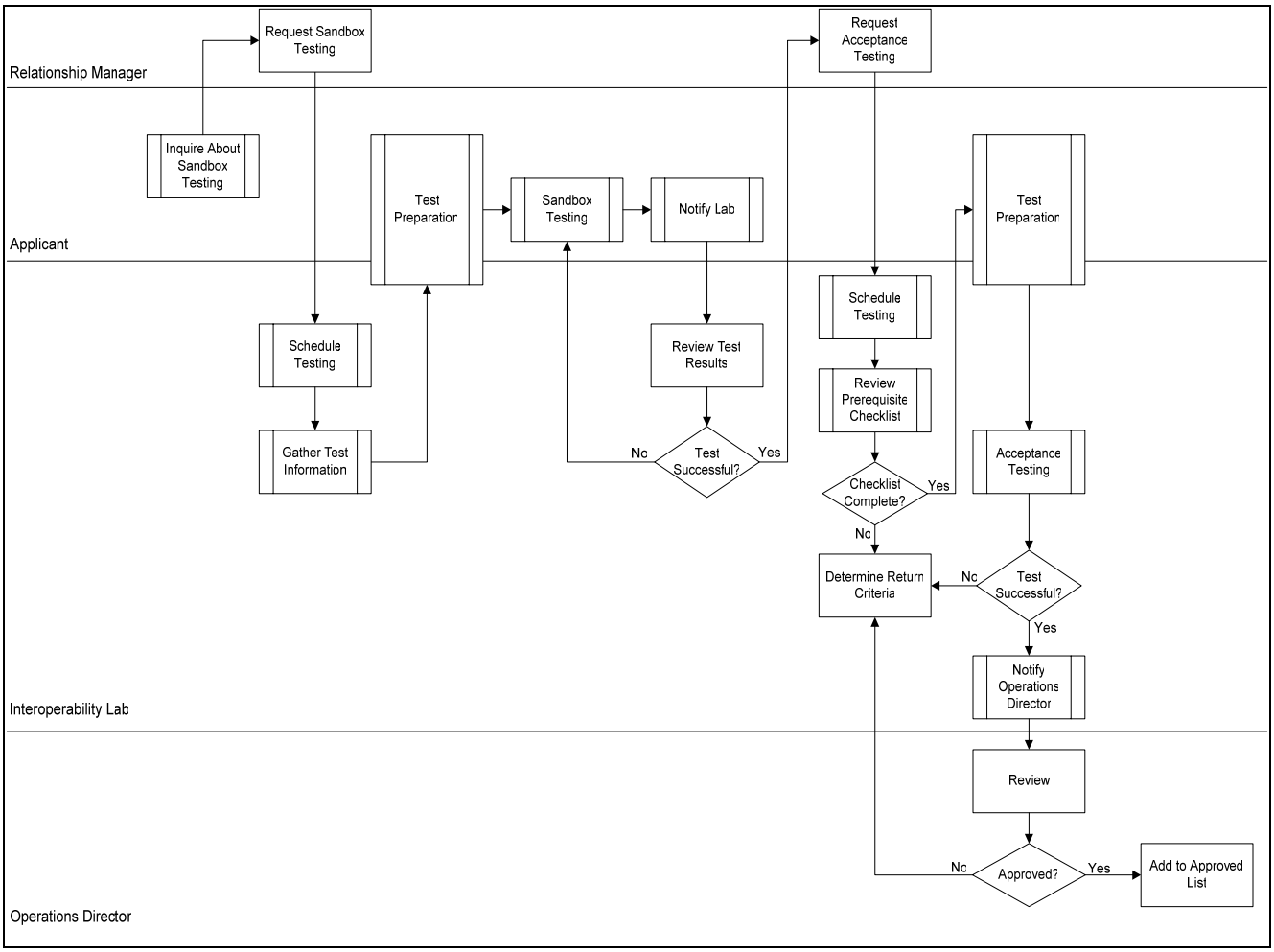
During testing of a new software product, a previously approved software product may be found incompliant with the *E-Authentication Interface Specifications*. If this occurs, the previously approved software product vendor or representative will be notified of the issue and given 15 business days to take corrective action. Furthermore, all Agencies and CSPs that have implemented the incompliant approved software product will be notified as well. The Program Executive has the authority to remove an incompliant approved software product from *The Approved E-Authentication Technology Provider List.*

5 Service Testing

5.1 Concept Overview

Figure 5 depicts the Lab's concept of operations for service testing of AAs and CSs.

Figure 5: Interoperability Lab Concept of Operations Process for Service Testing



This Lab concept is based on a collection of:

- Personnel, Staff and Organization (Section 3);
- Process and Activities;
- Guiding Principles and Practices (Section 8).

5.2 Service Testing Process

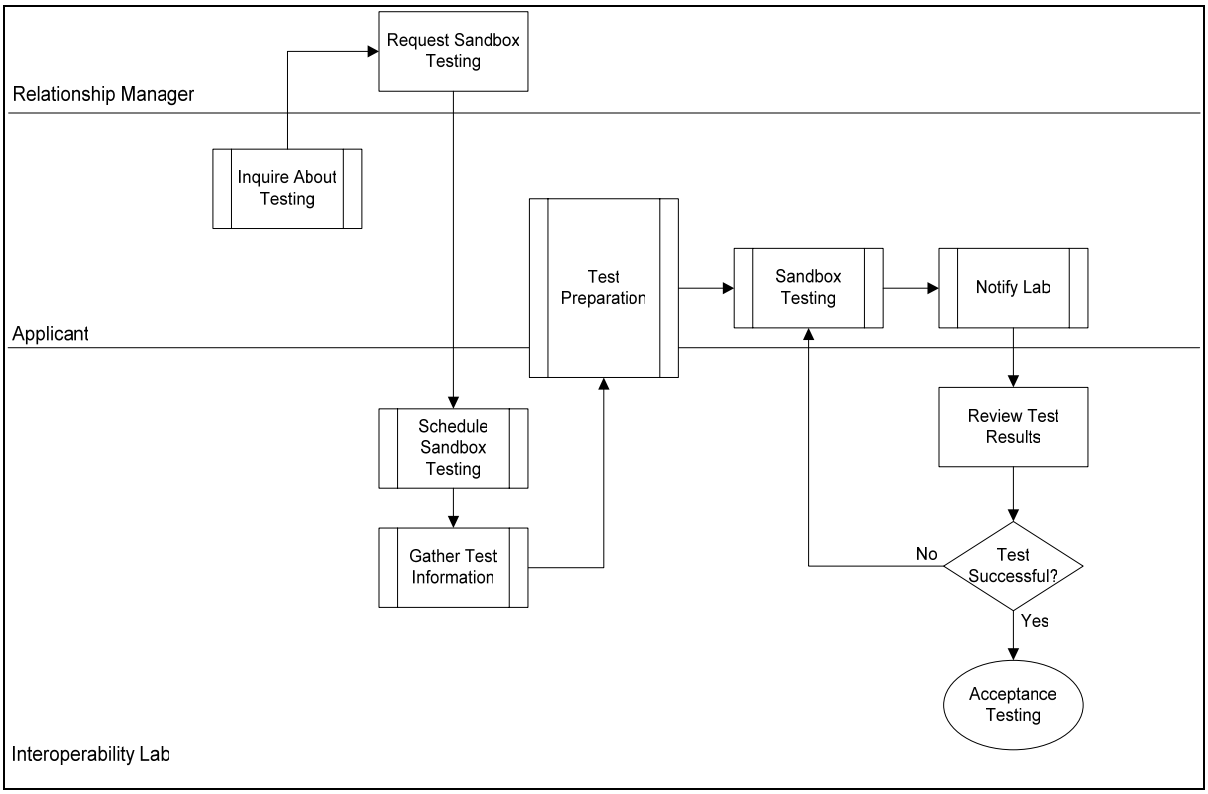
The following sections describe the steps involved with service testing of AAs and CSs. The two (2) testing processes used for service testing are:

1. Sandbox Testing Process;
2. Acceptance Testing and Approval Process.

5.2.1 Sandbox Testing Process

The process for Sandbox Testing is depicted in Figure 6 below.

Figure 6: Sandbox Testing Process



5.2.1.1 Inquire About Testing

The first step is for the Applicant (Agency or CSP) to contact their Relationship Manager for inquiring about Sandbox Testing. At this time, the Relationship Manager will answer any testing questions the Applicant may have.

5.2.1.2 Schedule Sandbox Testing

Once it has been determined that the service is prepared for Sandbox Testing, the Relationship Manager will request Lab time for testing. Upon receiving a testing request, the Lab Manager will schedule testing based on the priority assigned by the Operations Manager. 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, Relationship Manager, and Applicant Technical Representatives.

5.2.1.3 Gather Test Information

Before any testing can begin, the Applicant needs to obtain metadata and a test E-Governance Certificate Authority (E-GCA) certificate. To obtain this information, the Applicant must submit a request to the Technical Evaluation Team lead. Upon receipt of the request, the Technical Evaluation Team lead will provide the Applicant with the appropriate metadata and submit a request to the E-GCA for a test certificate. Once received, the Technical Evaluation Team lead will forward the test certificate to the Applicant.

5.2.1.4 Test Preparation

When all test information has been gathered, the Lab and Applicant will prepare for testing. In preparation for testing, the Technical Evaluation Team configures two (2) approved software products for the service to interoperate with. If requested by the Applicant, additional approved software products can be configured. These approved software products are chosen by the Technical Evaluation Team from *The Approved E-Authentication Technology Provider List*. The Technical Evaluation Team will perform additional Lab preparation tasks, including the configuration of metadata and installation of the test certificate. If requested by the Applicant, the Lab will place the service on a test Portal. The Applicant is responsible for the service configuration/preparation, although the Technical Evaluation Team is available for assistance.

5.2.1.5 Sandbox Testing

The Technical Evaluation Team provides a supportive role for Sandbox Testing, while the Applicant is responsible for executing the test procedures. If needed, the Technical Evaluation Team is available to provide additional support or assist with any questions the Applicant may have.

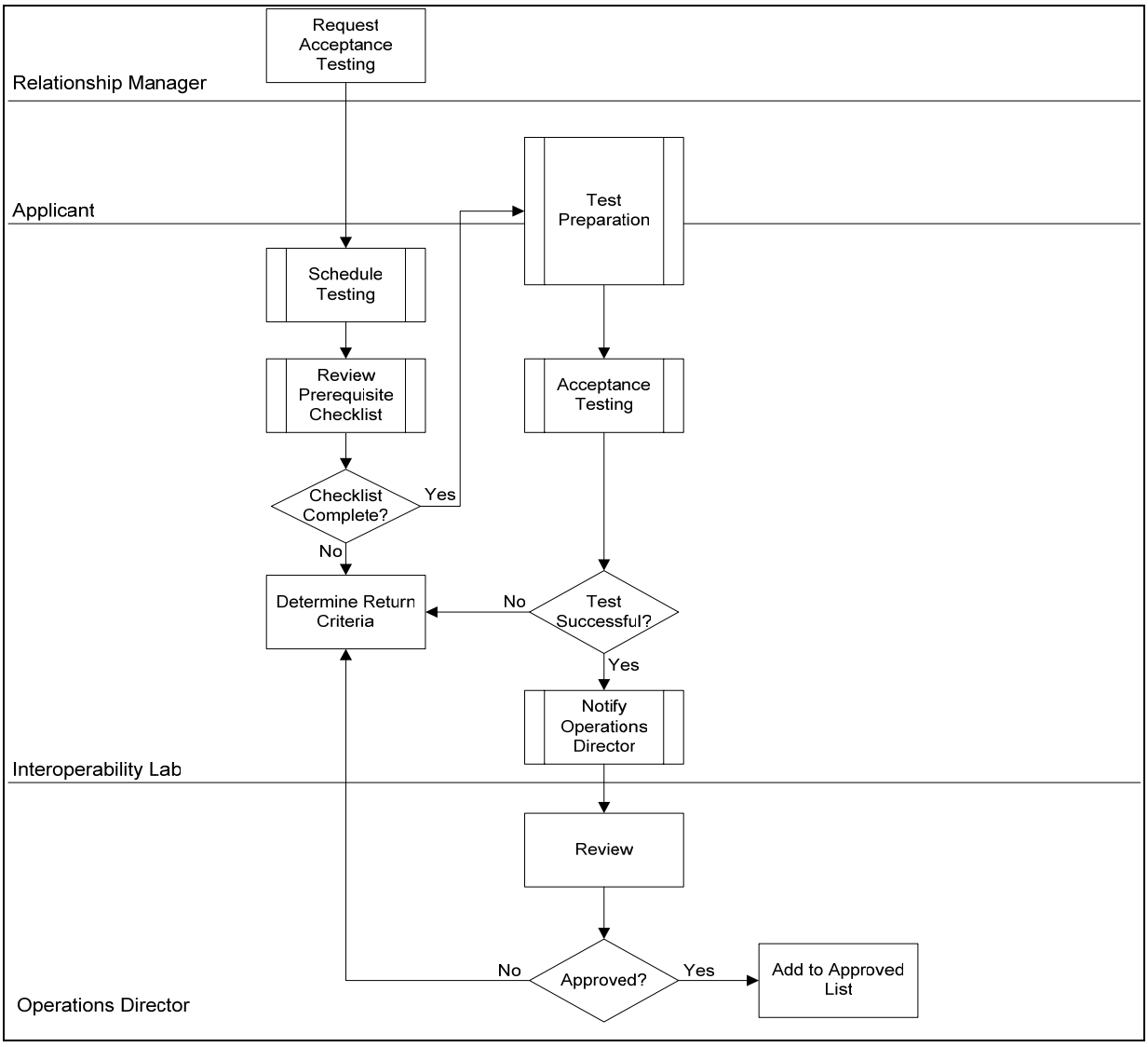
5.2.1.6 Interoperability Lab Notification

When an Applicant believes to have successfully interoperated with the configured approved software products, the Lab must be notified for test evaluation. The Technical Evaluation Team will review the test logs to ensure interoperability was successful. If it is determined that the test was not successful, the Technical Evaluation Team will notify the Applicant and provide the identified issue(s). Once the Lab has determined that testing was successful, the Applicant is notified and can participate in Acceptance Testing.

5.2.2 Acceptance Testing and Approval Process

The process for Acceptance Testing is depicted in Figure 7 below.

Figure 7: Acceptance Testing & Approval Process



5.2.2.1 Schedule Acceptance Testing

For the Acceptance Testing process to begin, the Applicant must contact their Relationship Manager for requesting Lab time for testing. Scheduling is handled as previously described in section 5.2.1.2. The Applicant is currently limited to two (2) weeks for Acceptance Testing.

5.2.2.2 Review Prerequisite Checklist

To ensure the service is properly configured for Acceptance Testing, the Technical Evaluation Team will meet with the Applicant to review and complete the *Prerequisite Checklist*. Before testing can begin services must meet all listed prerequisites.

5.2.2.3 Test Preparation

Once the Lab believes the service has been properly configured for testing, the Lab and Applicant will prepare for testing. In preparation for testing, the Lab will configure the service into the SAML Server and test Portal, ensure the E-GCA test certificate is properly configured, and prepare a test plan. The test plan is submitted to the Applicant for review. The Applicant is responsible for ensuring that the service is properly configured for testing and making any necessary modifications. For testing purposes, the service must be configured on a system equivalent to the Agencies "production environment".

5.2.2.4 Acceptance Testing

For Acceptance Testing, the Applicant cannot directly interact with testing; the Technical Evaluation Team will execute the tests, and collect and examine all available test data.

All Acceptance Testing results/issues are recorded and maintained by the Technical Evaluation Team. The Technical Evaluation Team will notify the Applicant at the completion of testing. When services have successfully completed Acceptance Testing, the Lab Manager will notify the Operations Director for official approval.

5.2.2.5 Operations Director Notification

The Operations Director makes the final approval decision, assigning:

Interoperable – Service meets all interoperability requirements and is added to the approved list.

Not Interoperable – Service does not meet interoperability standards and is not added to the approved list.

Once the final approval decision has been made, the Operations Director will notify the Applicant and, if approved, add the service to the appropriate approved list.

6 ASC Component Testing

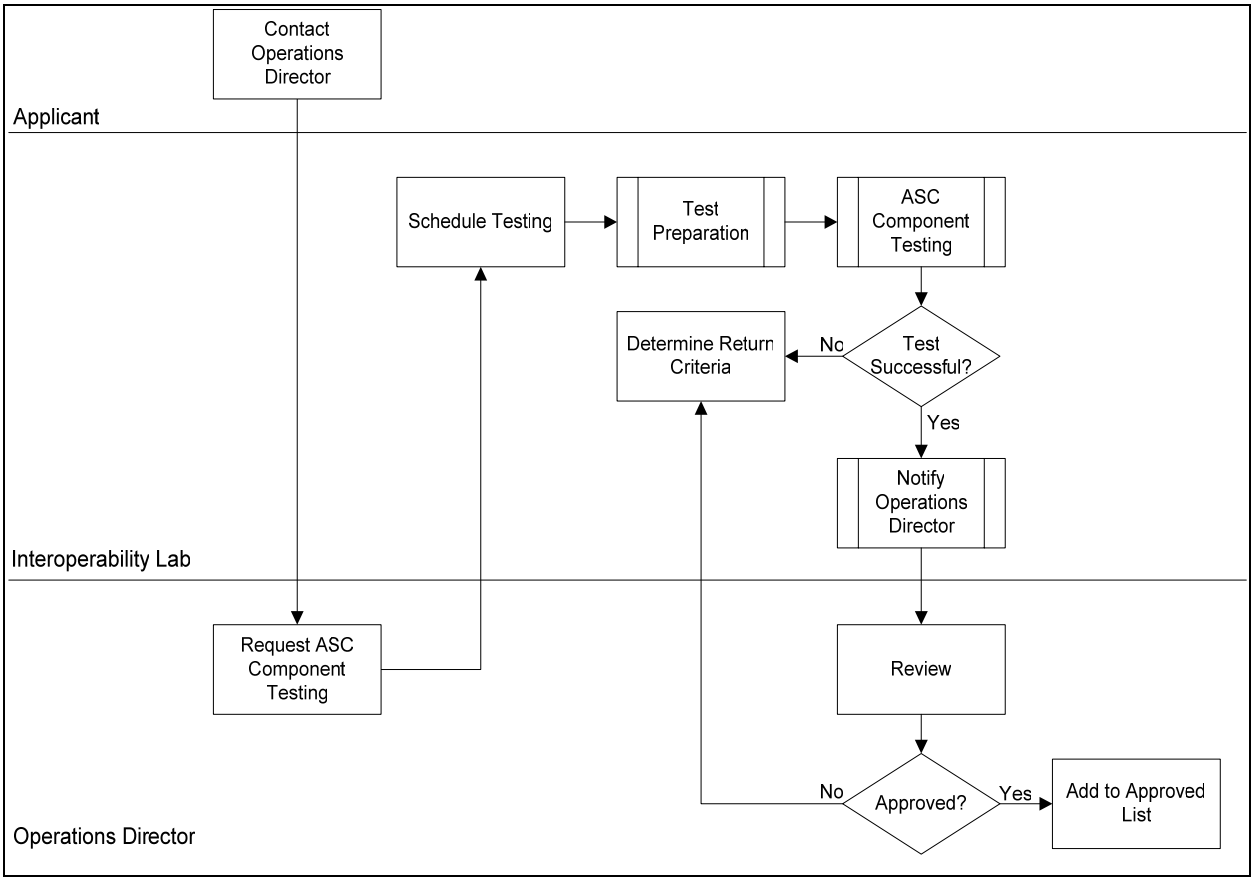
The following sections describe the steps involved with ASC component testing. This Lab concept is based on a collection of:

- Personnel, Staff and Organization (Section 3);
- Process and Activities;
- Guiding Principles and Practices (Section 8).

6.1 ASC Component Testing and Approval Process

The process for ASC component testing is depicted in Figure 8 below.

Figure 8: ASC Component Testing & Approval Process



6.1.1 Contact Interoperability Lab

The first step is for the Applicant (ASC Component Owner) to contact the Operations Director in regard to having an ASC component tested by the Lab. The Operations Director will then request Lab time for testing. Upon receiving the test request, the Lab Manager will schedule testing based on the priority assigned by the Operations Manager and assign resources. 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, and Applicant Technical Representatives.

6.1.2 Prepare for Testing

Once the ASC component has been scheduled for testing, the Lab and Applicant will prepare for testing. In preparation for testing, the Lab will prepare a test plan and submit it to the Applicant for review. The Applicant is responsible for ensuring that the ASC component is properly configured for testing and making any necessary modifications.

6.1.3 ASC Component Test

For ASC component testing, the Technical Evaluation Team will execute the tests, and collect and examine all available test data.

All ASC component testing results/issues are recorded and maintained by the Technical Evaluation Team. The Technical Evaluation Team will notify the Applicant when testing has been completed. When ASC components have successfully completed testing, the Lab Manager will notify the Operations Director for official approval.

6.1.4 Operations Director Notification

The Operations Director makes the final approval decision, assigning:

Interoperable – ASC component meets all interoperability requirements and is added to the approved list.

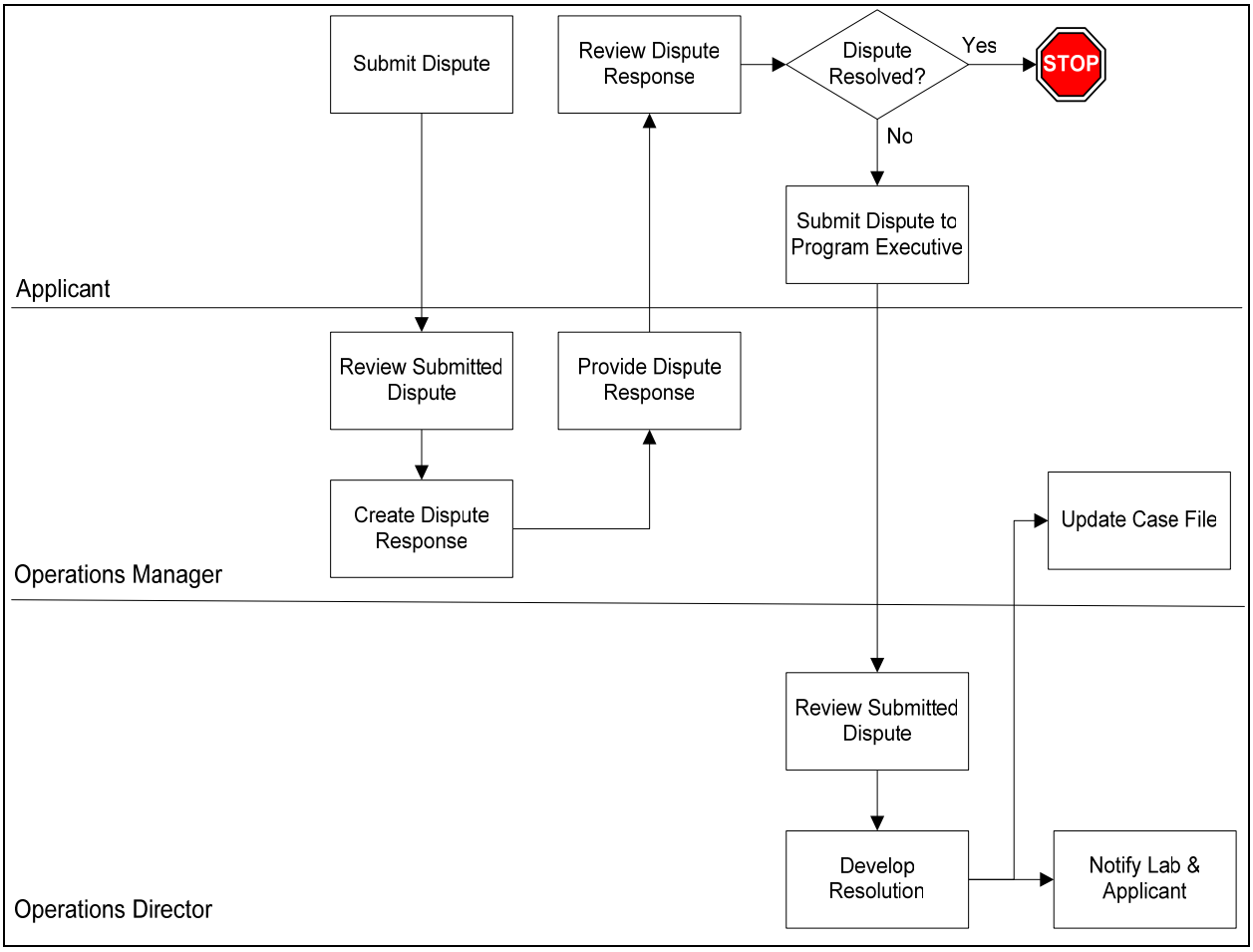
Not Interoperable – ASC component does not meet interoperability standards and is not added to the approved list.

Once the final approval decision has been made, the Operations Director will notify the Applicant and, if approved, add the ASC component to the appropriate approved list.

7 Dispute Resolution Process

The process of resolving disputes that arise between Applicants and the Lab is depicted in Figure 9.

Figure 9: Dispute Resolution Process



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

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

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

In some cases, the evaluation performed and the resolution developed by the Operations Director 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 software product.
3. Applicant believes its software product was not tested in a fair and ethical manner.
4. Applicant disagrees with the testing results.
5. Applicant disagrees with determination (situations in which the Lab tested the software product, service, or ASC component as fully interoperable, but the Operations Director decided not to add the software product to the approved list).
6. Applicant believes it should have more time, beyond the 15 days set forth by the Lab policies, to fix problems with its software product.

The Operations Director has final discretion on adding a software product, service, or ASC component to their appropriate approved list.

8 Guidance Principles and Practices

8.1 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 software product. For this reason, all software product vendors must sign the *Lab Service Agreement* to prevent the disclosure of proprietary information.

8.2 Scheduling

For software product testing, the Lab operates on a block schedule approach that allows the Lab to focus on a particular scheme or set of related software products. For example, April 1-20 might be dedicated to SAML 1.0, 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.

8.3 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 that are documented in the Lab Operations Manual.

Appendix A: Document History

Status	Release	Date	Comment	Audience
Release	1.0.0	07/30/04	Official release of document.	Limited
Revision	1.0.1	03/04/05	▪ Added section/sub-sections titles for AA and CS testing (CR #5). ▪ Added AA/CS testing information to Introduction section (CR #5). ▪ Made minor format changes. ▪ Added Lab Service Agreement to list of documents that are submitted by an applicant (CR #2).	Limited
Revision	1.0.2	03/08/05	▪ Provided text explaining that product vendors are only given 3 days for installation in section 4.2.2.1 (CR #3). ▪ Removed the use of conformance and replaced with compliant/compliance throughout document (CR #6). ▪ Added hosting of interoperability events to section 1.3 (CR #7). ▪ Added the Lab's role of writing, reviewing, and/or commenting upon architecture change requests and E-Authentication Specifications to sections 1.3 and 1.4 (CR #8). ▪ Added HSPD-12 to the policies and guidance bulleted list in section 2.1 (CR #9) ▪ Reworded last sentence in first paragraph of section 2.2 (CR #10). ▪ Clarified that As new types and versions of schemes are adopted by the Initiative, the need for additional testing grows (CR #11) ▪ Changed protocols to standards in section 2.2 (CR #12). ▪ Deleted Publication from the Services and Function table in section 1.4 (CR #14). ▪ Moved Services and Function section to Introduction section. ▪ Moved Roles and Responsibilities section to its own section. ▪ Changed Certification Testing to COTS Product Testing. ▪ Created a section titled "COTS Product Testing." ▪ Reworded the second paragraph in section 3.1 as it was difficult to read and follow (CR #15). ▪ Added PMO roles of review, approve, and prioritize, and add to approved list in section 3.6 (CR #16). ▪ Changed "Apply for Certification" to "Inquire about Certification" to diagram and sub-section header in section 4.2.1 (CR #18).	Limited

			▪ Reworded second paragraph of section 4.2.1.1 with "GSA may announce the commencement of testing a new scheme…" (CR #19) ▪ Provided teleconferencing with vendor to section 4.2.1.4 (CR#20). ▪ Clarified that it is an issue of the certified product against which the candidate product is being tested in section 4.2.2.1 (CR #21). ▪ Changed first box in dispute resolution diagram to "Submit Dispute" in section 6 (CR #22).	
Revision	1.0.3	03/16/05	▪ Added the process flow diagrams for sandbox and acceptance testing of AAs and CS (CR #5). ▪ Updated lab services diagram in Introduction section. ▪ Added sections and text describing sandbox and acceptance testing processes (CR #5).	Limited
Revision	1.0.4	03/25/05	▪ Change certified products and services to approved products and services (CR #22). ▪ Replaced COTS product testing with Software product testing, and replace AA/CS testing with services testing. Changes were made throughout the document (CR #24). ▪ Added section for ASC component testing, which included the addition of a process flow chart (CR #25). ▪ Removed the reference to the use of letters throughout the document. Document now specifies "notify" the Applicant (CR #26). ▪ Remove the reference to the Installation and Administration documentation throughout the document (CR #27). ▪ Removed "Agency Specific Testing" from Service and Function table. That is considered AA testing and is now covered in services testing (CR #28). ▪ Added roles and responsibilities for Program Executive, Operations Manager, and Operations Director (CR #29). ▪ Updated software testing and services testing figures to reflect operations manager and director roles (CR #30). ▪ Updated the dispute resolution section with roles of operations manager and operations director, which includes an update to the dispute resolution figure (CR #31). ▪ Added addition Lab services to the Interoperability Lab section and updated the services diagram accordingly (CR #32).	Limited
Revision	1.0.5	03/30/05	▪ Changed spelling of eGCA to E-GCA. ▪ Reworded sentence in regard to software product, service, and ASC component testing	Limited

			(CR #24). ▪ Added text describing that a software product must be FIPS approved, and that a copy of the FIPS Certification must be provided along with the application package (CR # 1).	
Revision	1.1.0	03/31/05	Release for update approval.	PMO
Revision	1.1.1	04/25/05	▪ Section 3.7. Changed scheduling of sandbox and acceptance testing to a lab manager responsibility (CR #33). ▪ Section 3.7. Added responsibility of providing AA/CS testing status for relationship managers (CR #34). ▪ Section 3.8. Added Ops Manager responsibility of providing agencies/CSPs with product waivers (CR #35). ▪ Section 3.9. Moved resolving unresolved disputes to an Ops Director responsibility (CR #36). ▪ Section 4.2.1.2 & 4.2.1.3. Removed the reference of applicants providing a copy of their FIP Certification. FIPS certification question will be asked in product questionnaire (CR #37). ▪ Section 4.2.2.4. Moved the software product verification letter request to after Ops Director is notified (CR #38). ▪ Section 6.1.1. Added step for specifying that the applicant contacts the Ops Director for ASC components to be tested (CR #39). ▪ Updated figures throughout document to reflect responsibility changes (CR #40).	Limited
Revision	1.2.0	04/26/05	Released to PMO for update approval.	PMO
Revision	1.2.1	05/11/05	▪ Section 2.3. Changed “Federal or commercial organization” to “Federal Agency” (CR #41). ▪ Moved document history to Appendix A (CR #42).	Limited
Release	2.0.0	06/06/05	Approved by the PMO.	Public