E-Authentication Handbook for Federal Government Agencies

Version 1.0.0
July 30, 2004

Executive Summary

This document presents general guidelines to government agencies planning to or already participating in the E-Authentication Initiative. The handbook provides a full life cycle view of E-Authentication participation, so as to provide agencies with complete perspective and guidance.

Table of Contents

1 Introduction

The E-Authentication Initiative will simplify secure interaction with Government Agencies through a trust network that links Agency Applications (Applications) and Credential Service Providers (CSPs). The E-Authentication Initiative assists those who are implementing E-Authentication techniques and services with a variety of resources, such as guidance, tools and technical information. This Handbook for Government Agencies offers guidance to Agencies regarding the E-Authentication Initiative, and helps you utilize the resources the E-Authentication Initiative provides.

This handbook provides wide coverage of topics that relate to Agencies, summarizing many of the requirements and specialized documents supporting the E-Authentication Initiative. Although the handbook provides guidelines and topic summaries, it is not intended to be an authoritative, comprehensive review of all specifications, agreements, or other documents. This document does not supersede or extend National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Office of Management and Budget (OMB) M-04-04, *E-Authentication Interface Specifications for the Security Assertion Markup Language (SAML) Artifact Profile, The Credential Assessment Framework (CAF*), or any Memorandum of Understanding (MOU) and/or a Memorandum of Agreement (MOA). The authors of the handbook will, whenever possible, relate the subject matter under discussion to any relevant document within the corpus of documents related to E-Authentication Initiative. For the entire library of E-Authentication documents, please visit http://www.cio.gov/eauthentication.

1.1 Purpose

This handbook is designed to assist Agencies in becoming E-Authentication enabled, which results in their becoming a member of the E-Authentication federation. This handbook is written and attended for Government Agencies that provide application services to end users. The ability to rely upon a definitive statement of who is interacting with an online Government Application is a cornerstone of E-Government. This handbook provides helpful guidelines for Agencies to understand the E-Authentication Initiative, the role of the Agency in the E-Authentication Initiative, steps involved in entering the community of trust, and the resources available to assist in that process. A companion Handbook for CSPs exists and focuses on similar information and guidelines for implementing Credential Services.

These handbooks are “living documents” and will be periodically updated to incorporate changes as needs of the E-Authentication Initiative and its participants evolve.

1.2 Document Organization

This handbook describes how Agencies should proceed throughout the full life cycle of E-Authentication Initiative participation. This handbook’s organization includes planning and implementing components of the E-Authentication Initiative and procedures used to accomplish many actions necessary to build a community of trust.

The document groups guidelines and recommendations based upon several helpful categories:

- E-Authentication Enabling Your Agency
- Implementation
- Operational Responsibilities

- Maintenance and Technical Evolution
- Resources

2 E-Authentication Enabling Your Agency

Agencies are vital partners in the success of E-Authentication and E-Government, as Agencies make available electronic services to enable quicker, more cost effective citizen-government interaction. The E-Authentication Initiative is pleased to welcome your agency's interest in supporting this critical transformation process, and looks forward to working with you.

2.1 Meet Your Agency Relationship Manager

In the spirit of partnership, the E-Authentication Initiative will designate an Agency Relationship Manager to collaborate with your Agency and help navigate the process to fully E-Authentication enable your Application. Agency Relationship Managers are Government employees working in the E-Authentication Program Management Office (PMO) and assigned by the Program Manager (PM) to coordinate all activities related to a given Application. Your Agency Relationship Manager will provide guidance and serve as one of your primary points of contact for the life of your relationship with the E-Authentication Initiative, which encourages Agencies, system owners and Agency Relationship Managers to maintain close contact and working relationships with one another to ensure open channels of communication.

2.2 Determine Your Application's Assurance Level

The government has outlined four levels of identity assurance per guidance from the OMB M-04-04 and its technical supplement document, NIST SP 800-63. As the system owner, you must assess the level of risk (i.e., level of identity assurance) you are willing to accept for your application. In this context, 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 the following potential impacts, outlined in OMB M-04-04:

1. Potential impact of *inconvenience, distress, or damage to standing or reputation*
2. Potential impact of *financial loss*
3. Potential impact of *harm to agency programs or public interests*
4. Potential impact to *personal safety*
5. Potential impact of *civil or criminal violations*

Additional potential impacts should also be considered, as appropriate, for your Application or Agency's overall mission.

The E-Authentication Initiative, in concert with the Software Engineering Institute (SEI) at Carnegie Mellon University, developed a tool to assist in the process. The tool, known as the E-Authentication Requirements and Risk Assessment tool (E-RA) is available online for download and is designed to facilitate the assessment of risks associated with a false positive authentication. Although the tool is not required, its use fulfils a requirement in the annual E-Government Act Report to OMB, required by section 202(g) of the E-Government Act, to report on Application assurance levels. Other factors, such as compensating controls, may help reduce the overall false-positive risk profile of your Application. The use of compensating controls may enable your Application to reduce the dependence on strength of the credential without significantly raising the risks of the system as a whole. Additional information on compensating controls is available on the E-Authentication Initiative website.

The PMO assesses Credential Services to determine their level of assurance. For more information on this assessment process refer to the Credential Assessment Framework (CAF). The Credential Service assurance level is then used by the E-Authentication Initiative to determine which Credential Services may be used to authenticate end users for access to the Application. Only Credential Services providing credentials corresponding to your Application's assurance level (or higher) are permitted to authenticate end users for access to your Application, thus ensuring that each Application's assurance level requirements are met.

2.3 Execute MOA/MOU with the E-Authentication Initiative

One of the final steps requires entering into a Memorandum of Understanding (MOU) and/or a Memorandum of Agreement (MOA) with the E-Authentication Initiative. The MOU/MOA covers roles, responsibilities, and any other necessary arrangements. The MOU/MOA will complete the process and formally establish an ongoing working relationship with the E-Authentication Initiative for you Agency. The MOU/MOA covers your commitments as an Agency, as well as the E-Authentication Initiative's commitment to your Agency.

3 Implementation

The implementation process will likely differ for each prospective Application, as it is dependent upon many factors such as assurance level, technical environment, vendor, and existing identity management. For assurance levels 1 and 2, Applications rely on assertion-based authentication, while levels 3 and 4 rely on certificate-based authentication. For more information on the different authentication approaches, see the *Technical Approach for the Authentication Service Component* in the E-Authentication Technical Suite.

3.1 Assertion Acceptance Implementations

The following notes focus on Agencies seeking to implement assertion-based authentication for one or more Applications. Agencies seeking to implement certificate-based authentication should refer to section 3.2 of this document.

For Applications operating at assertion-based authentication levels, the E-Authentication Initiative has published a suite of technical documents related to SAML implementation. The E-Authentication Technical Suite consists of three documents:

1. E-Authentication Interface Specifications for the SAML Artifact Profile
2. SAML Artifact Profile as an Adopted Scheme for E-Authentication
3. Technical Approach for the Authentication Service Component

These documents are available online for review at http://www.cio.gov/eauthentication.

3.1.1 Selecting an Interoperable Product

The E-Authentication architecture uses a federation of Credential Services and Applications, and relies on no single entity to provide or guarantee credentials. As such, each Agency is free to select from a variety of Commercial-off-the-Shelf (COTS) products implementing any combination of E-Authentication Initiative adopted schemes. Some COTS products may be a product suite. Depending upon Application system needs, the entire COTS product suite may need to be used. Participants may even develop their own "home grown" implementations of adopted schemes, as long as they comply with E-Authentication specifications for those adopted schemes.

Despite the existence of published E-Authentication specifications, it is quite possible and indeed likely that one or more Credential Service of Application implementations will not fully comply with the E-Authentication specifications. The result could be failure to interoperate within the E-Authentication system. To mitigate this risk, the E-Authentication Initiative has established an E-Authentication Interoperability Lab (Lab). The Lab's function is simple – verify the interoperability of all schemes, components, Agency Applications and Credential Services. All adopted scheme implementations, whether COTS or "home grown", must be certified as interoperable by the Lab prior to public use. The E-Authentication Initiative publishes a list of certified interoperable software online for the benefit of all participants, available at the E-Authentication website (see section 6). E-Authentication Initiative participants should select from this list to ensure the interoperability of their Credential Service or Application.

3.1.2 Implement a Test Capability

Applications are required to support test processing in the production environment as defined in section 3.2 of the *E-Authentication Interface Specifications for the SAML Artifact Profile*. Test processing enables the E-Authentication Initiative to verify the operational status of an Application, and facilitates acceptance of new systems into the operational federation. To facilitate testing, the E-Authentication Initiative has defined a uniform test processing mechanism required of all Applications.

Any assertion successfully transmitted to the Application that has the Assurance Level attribute set to "Test" must result in the Application displaying a page indicating the test was successful. The interface specifications require the page to contain certain elements such as the common name and Credential Service identifier (CSid). Please refer to section 3.2 of the *E-Authentication Interface Specifications for the SAML Artifact Profile* for more details.

The test capability must be permanent and part of the operational system. It is not a duplicate of an Application's full functionality; it is only a test interface to the SAML capabilities of the Application.

3.1.3 eGoverance Certification Authorities

The E-Authentication Initiative has established an eGovernance Certification Authority (eGCA) in which the scope is to issue certificates to Credential Services and Applications for use in assertion-based authentication. These certificates are for the servers, not for people. These certificates are necessary to ensure that only sanctioned organizations can participate in the federation. The eGCA operates three CAs. The first CA issues certificates to assurance level 1 CSPs. The second CA issues certificates to assurance level 2 CSPs. The third CA issues certificates to Applications. eGCAs also issue certificates for testing, as necessary.

Certificates from the eGCAs are the basis of a secure Simple Object Access Protocol (SOAP) channel that is used to pass SAML token and identity assertion between the Credential Service and Application. An Application should not interoperate with a Credential Service unless the Credential Service presents a certificate issued by the appropriate eGCA to secure the SOAP channel. For an overview of the role of the eGCA in the SAML hand-off, refer to the *SAML Artifact Profile as an Adopted Scheme for E-Authentication*, section 4.

Assertion-based Agency Applications will be required to obtain certificates from the appropriate eGCA. These certificates are used by the Credential Service to verify that the Application is part of the federation (i.e., trusted). Agencies will also need to install the eGCA self-signed certificates as trust anchors to verify that the Credential Service is part of the federation (i.e., trusted). Detailed recipes for the configuration of your product may be available in the *E-Authentication Cookbook*.

3.1.4 Secure SOAP Channel

At assertion-based authentication levels, the previous section mentioned that certificates issued by the eGCA are required for the TLS/SSL connection to secure the SOAP channel used to exchange the SAML artifact and identity assertion between the Credential Service and Application. The certificates enable each party (Credential Service and Application) to verify the identity of the other, and enable the transmission of the SAML artifact and identity assertion without tampering, as described in the *E-Authentication Interface Specifications for the SAML Artifact Profile*.

The following table indicates which eGCAs an Application is required to trust at assertion-based authentication levels (assurance levels 1 and 2). Level 2 Applications should only trust the level 2 eGCA, while level 1 Applications should trust both the level 1 and level 2 eGCAs. The third CA is a

test CA used to issue certificates for the interoperability testing (prior to approval to operate) and for operational tests of E-Authentication participants.

Table 1

	Application Assurance Level	
eGoverance CA	1	2
Level 1eGCA	√	X
Level 2 eGCA	√	√
Test eGCA	√	√
√ = Trust	X = Do Not Trust	

Agencies operating Applications at assertion-based authentication levels will be required to obtain certificates from the appropriate eGCA. The table below indicates which eGCAs issue certificates to Applications at specific assurance levels to secure the SOAP channel. An Application at either level 1 or level 2 should obtain a certificate from the Application CA. Again, the third CA is a test CA used to issue certificates for the interoperability testing (prior to approval to operate) and for operational tests of E-Authentication participants. Test assertions at the test level of assurance may be transmitted using the test CA certificates.

Table 2

	Application Assurance Level	
eGovernance CA	1	2
Level 1 eGCA	√	X
Level 2 eGCA	X	√
Test eGCA	√	√
√ = Required	X=Do Not Obtain	

Agencies will also need to install the eGCA self-signed certificates as trust anchors or the SOAP Responder to enable verification of the Credential Service certificates. Applications will also need to present the eGCA certificates issued to them during the TLS/SSL handshake to secure the SOAP channel. Detailed recipes for the configuration of your product may be available in the *E-Authentication Cookbook*.

3.1.5 Session Reset Mechanism

The SAML assertion provided by the Credential Service has two timestamps, one indicating when the assertion was created, and another indicating when the user authenticated. The SAML standard specifies requirements limiting the acceptable lifetime of the assertion, but policies on how recently the user was required to authenticate will vary across Credential Services[1].

If Applications have requirements on how recently a user authenticated, above and beyond what is required by the E-Authentication Initiative, there is a mechanism to request the Credential Service to re-authenticate the end user. This mechanism is referred to as *session reset*, and is described in section 3.1 of the *E-Authentication Interface Specifications for the SAML Artifact Profile.*

To request a fresher authentication, the Application redirects the end user back to the E-Authentication Portal (Portal) with special parameters on the query string. This mechanism should not be employed by default, but only used after inspection of the authentication timestamp. This mechanism is optional and only necessary if the session management requirements of NIST SP 800-63 and the CAF are deemed insufficient. Please notify your E-Authentication Agency Relationship Manager if you intend to use this mechanism.

3.2 Certificate-Based Implementations

The following sections focus on Agencies seeking to implement certificate-based authentication for their Applications. A primer on Public Key Infrastructure (PKI) concepts and the Federal PKI (FPKI) are outside the scope of this document, and the reader is assumed to have a working knowledge of these concepts for the following sections. Additional background and information is available from your E-Authentication Agency Relationship Manager and the E-Authentication Initiative website.

Accepting certificates for end user authentication requires validation of the certificate at two levels. The first level of validation verifies the issuing chain of certificate authorities (CAs) and includes an E-Authentication trusted CA. The second level of validation ascertains the certificate's status. Both of these steps are required.

The E-Authentication Initiative has worked closely with commercial product vendors to foster COTS support for technical elements of the E-Authentication Initiative. There may be validated products, technical recipes, or other helpful information available from your E-Authentication Agency Relationship Manager or the E-Authentication Initiative website.

There are three main considerations in configuring an Application for certificate-based authentication; (1) determination of Credential Service trust, (2) determination of certificate status, and (3) use of a Hint List. The following sections discuss each of these elements.

3.2.1 Determination of Trust

Software that implements certificate-based authentication has to be configured with some number of *Trust Anchors*. A trust anchor is a self signed root certificate issued by a CA. Trust anchors provide the basis of all trust decisions. An Application that has installed a particular CA's trust anchor will trust any certificate issued by that CA.

[1] NIST SP800-63 and the CAF place some limitations on session management at the Credential Service.

The E-Authentication Initiative maintains a list of CAs who are trusted[2] by the E-Authentication federation. Two technical options exist for your Application to determine trust at the time of authentication. One is to simply install the trust anchors for every CA on the E-Authentication Trust List, the other is called Certificate Path Discovery and Validation.

Certificate Path Discovery and Validation is the recommended approach. When the FPKI Policy Authority determines a CA is trustworthy, the Federal Bridge Certification Authority (FBCA) and the CA exchange cross-certificates. If anything goes wrong with the CA the FBCA can revoke that certificate and terminate trust. By looking for these certificates at run time, your Application can determine which CAs are currently trusted by the FPKI. Finding a chain of certificates from your agency's trust anchor through the bridge to the end user's issuing CA is referred to as Certificate Path Discovery and Validation. Processing certification paths is very complex and currently not widely supported in commercial products. The E-Authentication Initiative is working closely with commercial product vendors to foster support for this functionality in COTS products, so support is expected to increase over time. As products become available, the Lab will test them to validate proper functionality and publish a list of approved products. For current information on software availability for this approach contact your Agency Relationship Manager or refer to the E-Authentication Initiative website.

Installation of every trust anchor is an easier and more widely supported approach, but has some risks. In this approach you simply install a trust anchor for every CA on the E-Authentication Trust List[3], then your software has no need to discover and validate certificate chains. The approach does not rely on the FBCA at runtime, but rather relies on the CA roots that are installed in your trust list. If trust in a particular CA is revoked by the FBCA, you will have to manually remove the revoked CA's trust anchor from your Application. Revocation of trust from the FBCA is extremely rare, would be well publicized, and your Agency Relationship Manager would ensure you are notified. The other risk with this approach is that installation of trust anchors creates unconstrained trust. When the FBCA exchanges cross-certificates with approved CAs, those certificates often contain constraints that limit the types of certificates that are trusted. For example, trust of a federal Agency's CA may be constrained to employees of that agency. This practice is primarily precautionary, although such constraints are lost by installation of the trust anchors. For the near term this approach is considered acceptable within the E-Authentication Initiative, but Agencies should plan on migrating to full path discovery and validation as commercial products become available.

3.2.2 Certificate Status Checking

Software that implements certificate-based authentication must be configured to check certificate status at transaction time. Different CAs have different methods for publishing revocation information. Currently, every CA trusted by the E-Authentication Initiative supports either Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRL). Keep in mind that accessing revocation information using OCSP may require a client certificate, which should be set up before becoming operational. Information about how to access revocation information for each CA on the trust list is available on the E-Authentication Initiative website. Your Application must be configured to access revocation information for every trusted CA.

---

[2] The policies, procedures, and criteria used to determine assess CAs for use by E-Authentication are defined in the Credential Assessment Framework[2] (CAF). The CAF defers assessment of CAs to the FPKI Policy Authority (FPKI PA), which controls the Federal Bridge CA (FBCA). For more information on the FPKI PA and the FBCA see http://www.cio.gov/fpkipa/.

[3] Trust Anchors are sensitive; they are available out of band from your Agency Relationship Manager.

3.2.3 Hint Lists

Certificate-based authentication for websites is accomplished by using TLS/SSL. The TLS/SSL protocol part of the handshake requires the server to send a list of acceptable CAs to the end user's browser. The browser uses this list to help the end user select an appropriate certificate for authentication. The list of CAs is referred to as a *hint list*.

E-Authentication enabled web sites must configure the web server with an appropriate hint list in order for the Application to function properly. The list of CAs is available from the E-Authentication Initiative through your Agency Relationship Manager, but the configuration of hint lists varies from product to product. Configuration Recipes for the product you have selected may be available in the *E-Authentication Cookbook*, which is available on the E-Authentication Initiative website. For more information on the role of hint lists in the E-Authentication architecture, refer to the *Technical Approach for the Authentication Service Component*, section 3.

3.2.4 Agency Validation Service

An Agency may need to trust other CAs in addition to those trusted by the FBCA. The E-Authentication Initiative has designed a way for this to work seamlessly within the E-Authentication architecture. Agencies may establish their own internal certificate validation services, known as Agency Validation Services (AVS). An Agency simply needs to install the root certificates of those non-FBCA cross-certified CAs it wishes to trust as trust anchors in the AVS. Certificates presented to the Application for validation are then verified against the bridge and against the AVS. If either validation is successful, the Agency may proceed to grant access to the end user.

3.3 Agency Application Identifier

Each Application is issued a unique identifier within the E-Authentication system. This identifier, known as the AAid, provides all other services with a unique and incontrovertible way of referring to your Application. If your Application has multiple interfaces with different assurance levels, each will be assigned a unique AAid. The identifier is used with session reset requests described in section 3.1.4 of this handbook. It is also used when users are redirected to the Portal to select a Credential Service. The interface specifications contain complete coverage of how and when to use the AAid in your Application.

3.4 Logos, Graphics, and Branding

As a participant in the E-Authentication Initiative, you will be allowed to display a small E-Authentication logo on your Application website. The E-Authentication PMO will advise you of the proper, authorized usage of such images. Depending upon your MOU/MOA, you may also be entitled to use this image in other materials and settings as well.

The PMO will require the rights to use some of your graphics, images, or text linked to your Application elsewhere in the E-Authentication system (e.g., Portal, Credential Service). These graphics, images, or text will help establish consistent branding and messaging for your Application throughout the E-Authentication system, so that end users can easily identify your Application. Your MOU/MOA may also provide these images for use in other materials and forums.

3.5 Metadata

The E-Authentication Initiative publishes metadata about each participating Application and Credential Service. This metadata is updated whenever new Applications or Credential Services are enabled within the Portal. It is recommended that Applications and Credential Services update their local copy of the metadata on a periodic basis.

4 Operational Responsibilities

This section provides guidance on operational requirements related to the E-Authentication Initiative. E-Authentication technical specifications describe these requirements. Other requirements may be specified in the MOU/MOA. These requirements can include business processes, technical operations or implementations, or other topics of interest to both the Agency and the E-Authentication Initiative.

4.1 Prepare Agency Help Desk to Address E-Authentication Calls

There may be instances in which an end user contacts your Application Help Desk or technical support to report an issue.

Your Help Desk is not required to answer specific questions regarding the Portal or specific Credential Services. However, your staff must be familiar with your Application within the context of the E-Authentication system, and be capable of escalating general issues to your internal E-Authentication point of contact who should raise them as appropriate with the E-Authentication team. Please reference section 6 – "Helpful Resources" for E-Authentication points of contact.

A general education on a federated authentication environment is recommended for Help Desk staff. Help Desk analysts will need to be able to determine whether a problem is related to the Application or one of the trusted Credential Services. Knowledge of the Portal, and which Credential Services are applicable is also recommended, as is awareness of any special relationships with Credential Service(s).

4.2 Checking and Updating Server Credentials

To ensure smooth, continual operation of the E-Authentication system, the E-Authentication Initiative requires that all participants maintain valid credentials from the eGCA[4]. This requirement is outlined in section 2 of the *SAML Artifact Profile as an Adopted Scheme for E-Authentication*. If your credentials are approaching their expiration date, please be sure to contact your Agency Relationship Manager to coordinate the issuance of fresh certificates. If your certificates are compromised or expired, please alert your Agency Relationship Manager immediately.

The interface specifications require your Application to detect attempted SAML hand-offs without appropriate credentials. Please report these and any other security related events to your Agency Relationship Manager as soon as possible.

4.3 Federation Growth & Metadata

As a critical foundation element to E-Government, the E-Authentication Initiative is open to all Agencies and actively pursues partnerships with industry and potential CSPs. These efforts result in an ever-growing federation of Credential Services and Applications, which provides your end user base with additional credentials that will work with your Application. To manage and coordinate the federation, metadata is published to participants. The metadata provides important attributes such as assurance level and website URL. An initial set of metadata was used to configure your Application during implementation, but the metadata is updated continuously. Applications and Credential Services should update their local copy of the metadata on a periodic basis to maintain current information. For detailed information about the metadata used in the E-Authentication system, please refer to the *E-*

[4] For assertion-based authentication levels

Authentication Interface Specifications for the SAML Artifact Profile. An overview of the role of metadata in the architecture is provided in section 4 of *SAML Artifact Profile as an Adopted Scheme for E-Authentication.* Additional recipes on the use of metadata may be available in the *E-Authentication Cookbook*.

4.4 Server Clocks

Assertion-based authentication typically carries with it a duration during which the Credential Service advises the recipient the assertion is valid. The simplest example of this is via online banking – many end users are familiar with the "timeout" message if no activity occurs for a specified period of time. As the recipient of an assertion, you may elect to set identity refresh policies for your Application that require updated authentication prior to interacting with end users. To ensure proper compliance of these policies, you should use a time synchronization system such as a Network Time Protocol (NTP) to ensure proper server time calibration, thus properly interpreting the authentication instant timestamps and requesting refreshed credentials when appropriate.

To request a session reset and authentication refresh, please see section 3 of this document. For more information regarding session management in general, please refer to NIST SP 800-63 for guidance.

4.5 Interoperability

While the architecture is flexible and the E-Authentication Initiative aggressively tests to ensure interoperability, there is the possibility that end user access may be impaired due to misconfiguration or improper implementation. In order to minimize the impact of such an event on the greater federation, the Portal has the capability to disable specific Credential Service-Application pairs during problem periods. This enables the E-Authentication team, in conjunction with the CSP and Agency, to audit/troubleshoot the interoperability issue(s), and restore interoperability promptly. The E-Authentication architecture inherently supports this capability, requiring no changes on the part of any CSP or Agency. To facilitate such troubleshooting, the PMO may request, from time to time, Application audit logs for the purpose of investigating and correcting interoperability issues that may arise between parties in the federation. During such events, your organization may receive requests to provide support for efforts to address interoperability issues. Your MOU may also cover additional stipulations or requirements for interoperability, auditing, or periodic testing.

Section 3.1 of the *E-Authentication Interface Specifications for the SAML Artifact Profile* requires your system to detect interoperability issues at runtime and deal with them gracefully. Please notify your Agency Relationship Manager anytime the problems arise so that the Portal can be updated and the resolution process can begin.

4.6 Logos, Graphics, and Branding

As discussed in section 3.4, you will be allowed to display a small E-Authentication logo on your Application website. The E-Authentication PMO will advise you of the proper, authorized usage of such images. Depending upon your MOU/MOA, you may also be entitled to use this image in other materials and settings as well.

The PMO will also require the rights to use certain graphics, images, or text linked to your Application website elsewhere in the E-Authentication system (e.g., Portal, Credential Service). These graphics, images, or text will help establish consistent branding and messaging throughout the E-Authentication

system, so that users can easily identify your Application. Your MOU/MOA may also provision these images for use in other materials and forums.

5 Maintenance, Support, and Technical Evolution

All operational information systems undergo technology upgrades as a part of the lifecycle to maintain compatibility as technologies evolve. The E-Authentication Initiative recognizes that this occurs, and recognizes that many Agencies have planned methodologies for managing and planning technical evolution. To assist, the handbook highlights a few areas to review and keep in mind during the maintenance and technical evolution of your system.

5.1 Modifying Your Application URL

Please be sure to notify your Agency Relationship Manager in advance if the URL for your Application is to be changed. Upon notification, your Agency Relationship Manager will take the appropriate actions to update the URL in the E-Authentication metadata. The metadata is provided to all E-Authentication Initiative participants; updating your URL in the metadata will enable Credential Services to continue providing credentials for your Application. The Portal will also be updated with the new URLs.

5.2 Technology Assessment

It is good business practice to reassess information systems periodically to ensure they still are accomplishing their intended work, and are still providing positive return on investment. In an era of shrinking budgets, the pressure tends to be to extend the technology refresh cycle. Most private industry and Agency portfolio management processes include a technology assessment for refreshment consideration. Components of the E-Authentication solution should be covered in your portfolio review process, but as the E-Authentication Initiative is a very recent, these components may require a higher-frequency refresh cycle for the short term.

5.3 Integration Verification

The E-Authentication Initiative recommends that you conduct internal interoperability tests with new software or versions, related to the E-Authentication Initiative, prior to deployment within your production environment. Although the Lab verifies interoperability with other products that implement the same adopted scheme, it is unable to verify interoperability with your back-end systems. Therefore, any decision on the part of your Agency to upgrade systems must include verification that the Application will continue to function normally post-upgrade.

New Applications added to your infrastructure should also be tested for interoperability within the E-Authentication system. Your Agency Relationship Manager will coordinate any needed testing.

5.4 Technology Updates

Each E-Authentication Initiative participant must ensure that any technology updates or environment changes comply with E-Authentication Initiative requirements. Interoperability certification of adopted scheme COTS products is version specific. E-Authentication Initiative participants should use approved versions in production environments associated with the E-Authentication Initiative. Be sure to verify that the lab has validated new versions of your software product before they are installed.

When updating your Application in any manner that affects E-Authentication (e.g., your SAML product), please remember to notify your Agency Relationship Manager. Your Agency Relationship Manager will need to assess the situation and, if necessary, schedule an updated integration test with the Lab. Re-testing for interoperability is required to ensure that all E-Authentication Initiative participants have implemented and configured their systems correctly. Agency Relationship Managers try to stay familiar with the activities of their assigned Agencies to ensure they provide the best possible service. Informal notification to your Agency Relationship Manager regarding anything that affects the E-Authentication system is recommended.

5.5 Branding Related Updates

As discussed in section 4.6 of this document, branding-related information about your Application is installed in the Portal. The E-Authentication Initiative urges all Agencies to communicate any branding changes to their assigned Agency Relationship Manager as soon as possible. Updated copies of the electronic files may be required to make updates to the Portal.

6 Helpful Resources

This section lists many helpful resources and references that may be of use in planning, implementing, or operating your Application.

6.1 Documents and Tools

- The E-Authentication Initiative maintains a website to provide easy access to information about the E-Authentication Initiative. The website also hosts a repository of documents related to the E-Authentication Initiative, including copies of all referenced guidance, technical specifications, and contact information.

  Available at: http://www.cio.gov/eauthentication

  Available at: http://www.cio.gov/eauthentication/library

- OMB Guidance M-04-04, provides guidance regarding E-Authentication to federal Agencies, outlines the four levels of assurance, and describes the need for a credential assessment process, thus serving as the basis for the CAF.

  Available at: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

- NIST Special Publication 800-63, Draft Recommendation for Electronic Authentication, provides technical guidance to agencies implementing E-Authentication, and introduces the concept of levels of authentication assurance.

  Available at: http://www.cio.gov/eauthentication/documents/NISTsp800-63.pdf

- Credential Assessment Framework & Credential Assessment Profiles provide guidance to assessors and CSPs regarding the criteria necessary for each assurance level. The CAF also serves as guidance for the CSP application process.

  Available at: http://www.cio.gov/eauthentication/CredSuite.htm

- The E-Authentication Risk and Requirements Assessment (E-RA) provides Agencies with a guide to assist in selecting the appropriate level of authentication for their Application.

  Available at http://www.cio.gov/eauthentication/documents/eraguide.pdf

- The E-Authentication Credential Service Provider Trust List contains the list of trusted CSPs developed by the PMO.

  Available at http://www.cio.gov/eauthentication/documents/TCSP.pdf

- The E-Authentication Technical Suite provides guidance and specifications regarding the overall technical approach, adopted schemes, and interfaces.

  Available at: http://www.cio.gov/eauthentication/library.htm

- The Approved E-Authentication Technology Provider List contains all certified interoperable vendor suites and applicable versions for use in the implementation of E-Authentication adopted schemes.

  Available at: http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm

Appendix A: Acronyms and Abbreviations

Acronym	Description
AA	Agency Application
AAid	Agency Application Identifier
AVS	Agency Validation Service
CA	Certification Authority
CAF	Credential Assessment Framework
CAP	Credential Assessment Profile
COTS	Commercial off the Shelf
CRL	Certificate Revocation List
CS	Credential Service
CSid	Credential Service Identifier
CSP	Credential Service Provider
eGCA	eGovernance Certification Authority
E-RA	E-Authentication Risk and Requirements Analysis
FBCA	Federal Bridge Certification Authority
FPKI	Federal Public Key Infrastructure
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
SAML	Security Assertion Markup Language
SEI	Software Engineering Institute
SOAP	Simple Object Access Protocol
SP	Special Publication
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Universal Resource Locator