



E-Authentication Handbook for Credential Service Providers

Version 1.0.0
July 30, 2004

Executive Summary

This document presents general guidelines to private industry organizations and government agencies interested in providing Credential Services for the E-Authentication Initiative. The handbook provides a full life cycle view of E-Authentication participation, so as to provide Credential Service Providers (CSPs) with complete perspective and guidance.



Table of Contents

1	Introduction.....	1
1.1	Purpose.....	1
1.2	Document Organization	1
2	Becoming an E-Authentication CSP.....	3
2.1	Meet Your Credential Manager	3
2.2	Assurance Levels	3
2.3	Credential Service Assessment	3
2.3.1	Assessment Package	4
2.3.2	Credential Service Assessment.....	4
2.3.3	Post Assessment	4
2.4	Memorandum of Understanding & Agreement	5
3	Implementation	6
3.1	Assertion Acceptance Implementations	6
3.1.1	Selecting an Interoperable Product.....	6
3.1.2	Implement a Test User Interface.....	7
3.1.3	eGovernance Certification Authorities	7
3.1.4	Secure SOAP Channel.....	7
3.1.5	Session Reset Mechanism.....	7
3.1.6	Metadata	8
3.1.7	Interoperable Configuration.....	8
3.2	Certificate-Based Authentication Implementations	8
3.2.1	Certificate Status Capability	8
3.3	Images, Graphics, & Logos.....	9
3.4	Credential Service Identifier	9
4	Operational Responsibilities.....	10
4.1	Prepare CSP Help Desk to Address E-Authentication Calls.....	10
4.2	Checking and Updating Server Credentials	10
4.3	Federation Growth & Metadata	10
4.4	Server Clocks	11
4.5	Interoperability.....	11
4.6	Logos, Graphics, and Branding.....	11
4.7	Single Sign-on.....	12
4.8	Implement a Test User Interface	12
5	Maintenance, Support, and Technical Evolution.....	13
5.1	Modifying Your Credential Service URL.....	13
5.2	Technology Assessment.....	13
5.3	Integration Verification.....	13
5.4	Technology Updates	13
5.5	Branding Related Updates	14
5.6	Credential Service Maintenance	14
6	Helpful Resources.....	15
6.1	Documents and Tools.....	15
	Appendix A: Acronyms and Abbreviations	16

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 offers guidance to CSPs regarding the E-Authentication Initiative, and helps you utilize the resources the E-Authentication Initiative provides.

The handbook is designed to provide wide coverage of topics that relate to CSPs, 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, the *E-Authentication Interface Specifications for the 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 documents 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 will help you plan for and participate in the community of trust the E-Authentication Initiative is building. This handbook is written and intended for CSPs that issue or register tokens (e.g., passwords, PINs, smart cards, certificates, etc.) and issue electronic credentials (e.g., PKI digital certificates) to end users. The ability to provide a definitive statement of who is interacting with an online government Application is a cornerstone of E-Government. This handbook provides helpful information and guidelines for CSPs to understand the E-Authentication Initiative, their role in the E-Authentication Initiative, steps involved in entering the community of trust, and the resources available to assist in that process. The handbook, in its entirety, is intended to walk the reader through the full life cycle of the engagement and highlight relevant, important elements within each phase. There is also a companion E-Authentication Handbook for Government Agencies focused on similar information and guidelines for implementing Applications.

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

1.2 Document Organization

This handbook describes how CSPs that issue or register tokens and issue credentials integrate the E-Authentication system. The handbook’s organization follows the engagement lifecycle and covers many details, procedures, and considerations for participation in the E-Authentication Initiative.

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

- Becoming an E-Authentication Credential Service Provider
- Implementation
- Operational Responsibilities

- Maintenance and Technical Evolution
- Resources

2 Becoming an E-Authentication CSP

The CSP is a vital partner in the success of E-Authentication and E-Government, as CSPs make available the realm of identity tokens and credentials that enable electronic citizen-government interaction with various levels of identity assurance. The E-Authentication Initiative is pleased to welcome your organization's interest in supporting this critical transformation process, and looks forward to working with you.

2.1 Meet Your Credential Manager

In the spirit of partnership, the E-Authentication Initiative will designate a Credential Manager to partner with your organization and help you navigate the process of becoming a certified and operational E-Authentication Initiative CSP. Credential 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 specific Credential Service. Your Credential Manager will provide guidance during the application process, schedule the credential assessment, and serve as one of your primary points of contact for the duration of your relationship with the E-Authentication Initiative. The E-Authentication Initiative encourages CSPs and Credential Managers to maintain close contact and working relationships with one another to ensure open channels of communication.

2.2 Assurance Levels

In the E-Authentication architecture, each CSP implements, manages, and maintains credentialing processes and or procedures that support their organizational needs. Some organizations require stringent identity verification prior to issuing credentials, while others may require less. While each organization plays a valuable role in providing those credentials for use with the government, the level of assurance provided by their identity policies is not the same.

The government has accordingly outlined four levels of identity assurance in guidance from the OMB M-04-04 and its technical supplement, NIST SP 800-63. This guidance was incorporated into the CAF. Prior to receiving final approval to operate, each Credential Service is assigned an assurance level as determined by the credential assessment.

Applications are accessible by end users with credentials whose assurance level is equal to or higher than the assurance level required by the Application. If you wish to make your credentials of your Credential Service's usable with an Application that requires a higher assurance level, you should review the CAF to identify and address the gap between your Credential Service's current assurance level and the Application's assurance level.. Once those gaps are addressed via policy, procedure, or technical implementation, as appropriate, contact your Credential Manager to schedule a re-assessment.

2.3 Credential Service Assessment

One of the most important steps to becoming an E-Authentication Initiative CSP is to participate in a credential assessment with the PMO for each proposed Credential Service. This collaborative process seeks to assess the assurance level of the credentials of the proposed Credential Service. To ensure a structured, consistent assessment, the E-Authentication Initiative has developed the CAF, which defines the policies, procedures, and criteria for assessing Credential Services. The CAF is based upon OMB

M-04-04 and NIST SP 800-63. To obtain the latest copy of the CAF or request clarification, please see <http://www.cio.gov/eauthentication/CredSuite.htm> or contact your Credential Manager.

At a high level, there are four main steps within the CAF:

1. Application for Assessment. Interested CSPs must prepare and submit the Application for Assessment.
2. Assessment Package. Assessment packages are prepared and submitted by the CSP upon acceptance of the Application for Assessment by the CEWG¹.
3. Credential Service Assessment. When the assessment begins, the CSP must present evidence that demonstrates compliance with any element of the Assessment Package not independently audited by a recognized auditor.
4. Credential Service Maintenance. Once a Credential Service becomes part of the E-Authentication Trusted Credential Service Providers (TCSP) list, certain maintenance activities are required by the CAF. (See Section 3.2.8 of the CAF for more information.)

2.3.1 Assessment Package

As part of the assessment process, CSPs will need to submit an Assessment Package containing Evidence of Compliance for each criterion in the applicable Credential Assessment Profiles (CAP). Evidence submitted may include results from an independent audit by a recognized auditor within the past year, and need only be sufficient in demonstrating compliance with relevant criteria. In other words, just enough information is required for the Assessment Team to make an informed decision on each criterion. For detailed information regarding the assessment package, please see section 3.2 of the CAF.

2.3.2 Credential Service Assessment

The Assessment Team will assess the evidence of compliance included in the assessment package against the criteria established in the applicable CAPs. Compliance with each applicable criterion will be determined by reviewing the appropriate Evidence of Compliance from the Assessment Package, and by determining its sufficiency with regard to the criterion. An intrusive audit of the Credential Service is not required so long as sufficient evidence of criteria compliance is provided in the assessment package.

2.3.3 Post Assessment

Upon approval from the Program Manager, you will need to enter into a service agreement prior to your Credential Service being included in the E-Authentication Trusted Credential Service Providers (TCSP) list. Once this agreement is in place, metadata describing your Credential Service is added to the E-Authentication Portal (Portal) and is available to all E-Authentication participants. Enabling your Credential Service at the Portal in this manner enables the use of your Credential Service's credentials at Applications with equal or lower assurance levels.

¹ The Credential Evaluation Working Group, as defined by section 2.2.7 of the Credential Assessment Framework

Depending upon the needs of the Government, your Credential Manager may request an annual review of your credential assessment. More frequent reviews of your credential assessment may be required if policy, procedure, or technical environment changes occur within your Credential Service. If your organization elects to make any changes to policies, procedures, or technical environments that affect your Credential Service, you are required to notify your Credential Manager. Your Credential Manager will coordinate the necessary updates or procedures with your designated primary point of contact.

2.4 Memorandum of Understanding & Agreement

Upon review and approval of your credential assessment results by the PM, your organization is almost ready to become an operational CSP. One of the final steps requires entering into service agreements, in the form of a MOU and/or a MOA with the PMO. The MOU/MOA will cover roles, responsibilities, and any other arrangements necessary; as such, it may add additional requirements not covered in the CAF. The MOU/MOA will complete the process and formally establish an ongoing working relationship with the E-Authentication Initiative.

3 Implementation

The implementation process will likely differ for each prospective Credential Service, as it is dependent upon many factors such as assurance level, technical environment, vendor, and existing identity management. For assurance levels 1 and 2, Credential Services use assertion-based authentication, while levels 3 and 4 use 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 CSPs seeking to implement assertion-based authentication for one or more Applications. Credential Services issuing certificate-based authentication should refer to section 3.2 of this document, entitled “Certificate-based Authentication Implementations”.

For Credential Services operating at assertion-based authentication levels, the E-Authentication Initiative has published a suite of technical documents related to Security Assertion Markup Language (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*

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 participant 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 Credential Service system needs, the entire COTS product 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 Initiative specifications for those adopted schemes.

Despite the existence of published E-Authentication Initiative specifications, it is quite possible and indeed likely that one or more Credential Service or Application implementations will not fully comply with E-Authentication Initiative 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 interoperability of all schemes, components, 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 Initiative website (see section 6). E-Authentication Initiative participants should select COTS products from this list to ensure the interoperability of their Credential Service or Application.

3.1.2 Implement a Test User Interface

Credential Services are required to support test processing in the production environment. Test processing enables the E-Authentication Initiative to verify the operational status of a Credential Service without requiring the maintenance of a local identity on the Credential Service. CSPs must implement several test accounts within each Credential Service, each of which must be assigned an assurance level of “Test”. All test accounts and passwords must be made available to the PMO, and system administrators should only have the rights to modify test accounts. Details on the test interface are in the *E-Authentication Interface Specifications for the SAML Artifact Profile*, section 2.3.

The test capability must be permanent and part of the operational system. It is not a duplicate of the full Credential Service; it is only a test interface to the SAML capabilities of the Credential Service.

3.1.3 eGovernance Certification Authorities

The E-Authentication Initiative has established the eGovernance Certification Authority (eGCA) to issue certificates to Credential Services and Applications for use in assertion-based authentication. These certificates are for the servers, not for people. They 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 Credential Services. The second CA issues certificates to assurance level 2 Credential Services. 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 the SAML artifact and identity assertion between the Credential Service and Application. Credential Services should not send assertions to Applications unless certificates from the eGCA are used 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.

3.1.4 Secure SOAP Channel

At assertion-based authentication levels, certificates issued by the eGCA are required for the TLS/SSL connection to secure the SOAP channel used in communicating 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*. Despite the authentication level, Credential Services only trust eGCA for Agency Applications.

Credential Services operating at assertion-based authentication levels will be required to obtain certificates from the appropriate eGCA according to their assurance level.

You will also need to install the eGCA self-signed certificates as trust anchors for the SOAP Responder to enable verification of the Application certificates. Credential Services will also need to present their eGCA certificate during the SSL/TLS 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 Services².

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 user. This mechanism is referred to as *session reset*, and is described in the E-Authentication Technical Suite.

The interface specifications for E-Authentication require your Credential Service to support this mechanism. Refer to section 2.1 of the *E-Authentication Interface Specifications for the SAML Artifact Profile* for more details.

3.1.6 Metadata

The E-Authentication Initiative publishes metadata that encapsulates information about each Credential Service and Application participating in the E-Authentication Initiative. This metadata is updated whenever new Credential Services or Applications are enabled within the Portal. While the architecture ensures that such events require no special handling at the Credential Service or Application, it is recommended that Credential Services and Applications update their local copy of the metadata on a periodic basis. Doing so will enable your Credential Service to provide additional uses for its credentials to your users.

3.1.7 Interoperable Configuration

In addition to the list of interoperable software, the E-Authentication Initiative also issues updates to the Cookbook containing new or updated recipes for configuring interoperable products. These recipes will assist the staff of CSPs and Agencies in the proper installation and configuration of the software to ensure interoperability. The E-Authentication Initiative also publishes a list of primary points of contact for each vendor and encourages any participants to contact the vendor's representative with questions about the product.

3.2 Certificate-Based Authentication Implementations

The following notes focus on CSPs seeking to use certificate-based authentication for one or more Credential Services. CSPs seeking to implement assertion-based authentication should refer to section 3.1 of this document, entitled "Assertion-based Authentication Implementations".

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

3.2.1 Certificate Status Capability

Certificate status information must be available online using either Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRL). Credential Services are required to provide their Credential Manager with the Universal Resource Locator (URL) for revocation information, and to

² NIST SP800-63 and the CAF place some limitations on session management at the CS

notify them of any changes or updates. If OCSF Responders require requestor certificates procedures and points of contact for obtaining them, then procedures and points of contacts for obtaining these certificates must be provided to the Credential Manager and must remain current.

3.3 Images, Graphics, & Logos

As an approved CSP and participant in the E-Authentication Initiative, you will be requested to provide rights for the display and use of your logo in association with E-Authentication Initiative materials, including the Portal. Such use communicates to the public the reusability of your Credential Service's credentials, and provides an easy, familiar way for end users to select your Credential Service at the Portal when presented with a list of applicable Credential Services. Please work with your Credential Manager to provide the necessary rights, permissions, and image file in support of your role as an E-Authentication Initiative CSP.

3.4 Credential Service Identifier

Per the use cases outlined in the Technical Approach for the Authentication Service Component document, each approved Credential Service is issued a unique identifier within the E-Authentication system. This identifier, known as the Credential Service id, provides all other services with a unique and incontrovertible way of referring to various Credential Services. As a CSP, you may operate multiple, distinct Credential Services. Each of these Credential Services will be assigned a separate Credential Service id.

4 Operational Responsibilities

This section provides guidance on operational requirements related to the E-Authentication Initiative. E-Authentication Initiative technical specifications describe these requirements. Other requirements may be specified in the MOU/MOA, which may also incorporate a Service Level Agreement (SLA). These requirements can include business processes, technical operations or implementations, or other topics of interest to both a CSP and the E-Authentication Initiative.

4.1 Prepare CSP Help Desk to Address E-Authentication Calls

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

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

A general education on a federated authentication environment is recommended for helpdesk staff. Help Desk analysts will need to be able to determine whether a problem is related to an Application or the Credential Service. Knowledge of the Portal, and which Applications rely on your credentials is also recommended. Any special relationships to supply specific Applications with credentials should also be communicated to your help desk staff.

4.2 Checking and Updating Server Credentials

Credential Services providing assertion-based authentication are required to have valid credentials from the eGCA³. 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 Credential Manager to coordinate the issuance of fresh certificates. If your certificates are compromised or expired, please alert your Credential Manager immediately.

The E-Authentication interface specifications require your Credential Service to detect attempted SAML hand-offs without appropriate credentials. Please report these and any other security related events to your Credential 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 user base with additional applications that will work with your credentials. To manage and coordinate the federation, metadata is published to all participants. Metadata provides important attributes such as assurance level and website URL. An initial set of metadata was used to configure your system during implementation, but the metadata is updated continuously. Applications and Credential Services should update their

³ For assertion-based authentication levels

local copy of the metadata on a periodic basis to gain maintain current information. For detailed information about the metadata used in the E-Authentication Initiative, please refer to the *E-Authentication Interface Specifications for the SAML Artifact Profile*. An overview of the role of metadata in the architecture is provided in section 4 of the *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

Credential Services should ensure their system clocks are correct and employ a time synchronization solution such as Network Time Protocol (NTP). Certificate revocation information, as well as SAML assertions both, contains timestamps that must be accurate.

4.5 Interoperability

While the architecture is flexible and the E-Authentication Initiative aggressively tests for interoperability, a possibility may occur 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 and troubleshoot the interoperability issue(s), and restore interoperability promptly. The architecture inherently supports this capability, requiring no changes on the part of any CSP or Agency participants. To facilitate such troubleshooting, the PMO may request, from time to time, Credential Service 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 handle with them gracefully. Please notify your Credential Manager anytime 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 Credential Service website. The 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 Credential Service website elsewhere in the E-Authentication systems (e.g., Portal, Application). These graphics, images, or text will help establish consistent branding and messaging between components within the E-Authentication system, so that users can easily identify your Credential Service. Your MOU/MOA may also provision these images for use in other materials and forums.

4.7 Single Sign-on

Seamless single sign-on must be supported as described by the *Technical Approach for the Authentication Service Component*. End users must opt-in to single sign-on, but the feature must always be available. Refer to the section 2.2 of the *E-Authentication Interface Specifications for the SAML Artifact Profile* for more details.

4.8 Implement a Test User Interface

Credential Services are required to support test processing in the production environment. Test processing enables the E-Authentication Initiative to verify the operational status of a Credential Service without requiring the maintenance of a local identity on the Credential Service. CSPs must implement several test accounts within each Credential Service, each of which must be assigned an assurance level of “Test”. All test accounts and passwords must be made available to the PMO, and should only be modifiable by the system administrator. If a Credential Service issues certificate-based credentials, a set of credentials may be required to test revoked, expired, and valid statuses. These credentials must be protected as if they pertain to a valid user to prevent misuse. If the “valid” test credentials expire, a non-expired test credential will need to be issued in its place so that the test interface can be maintained.

At assertion-based authentication levels, certificates issued by the eGCA are required for the TLS/SSL connection to secure the SOAP channel used in communicating the SAML artifact and identity assertion between the Credential Service and Application. To verify that the Application is a trusted E-Authentication Initiative participant, Credential Services operating at assertion-based authentication levels are required to trust the specific eGCA.

All CAs issue certificates for interoperability testing, which is done prior to approval to operate, and for operational tests of E-Authentication Initiative participants

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 CSPs have planned methodologies for managing and planning technical evolution. To assist, the authors of the handbook have highlighted a few areas to review and keep in mind during the maintenance and technical evolution of your system.

5.1 Modifying Your Credential Service URL

Please be sure to notify your Credential Manager in advance if the URL for your Credential Service is to be changed. Upon notification, your Credential 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 the E-Authentication system to continue using your Credential Service. 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 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 organization to upgrade systems must include verification that the Credential Service will continue to function normally post-upgrade.

New or replacement Credential Service servers added to your infrastructure should also be tested for interoperability within the E-Authentication system. Your Credential 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 for 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 before they are installed.

When updating your Credential Service in any manner that affects the E-Authentication system (such as your SAML product), please remember to notify your Credential Manager. Your Credential 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 participants have implemented and configured their systems correctly. Credential Managers try to stay familiar with activities at their assigned CSPs to ensure they provide the best possible service. Informal notification regarding anything that may effect the authentication related aspects of your system is recommended.

5.5 Branding Related Updates

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

5.6 Credential Service Maintenance

As a CSP, you are relied upon to provide credentials to users wishing to interact with online Federal Government services. Your existing credential provisioning may include options for systems maintenance (e.g., downtime, patch installation). Additional options or agreements regarding maintenance for your Credential Service (s) may also be incorporated into the MOU/MOA via an SLA or individual clauses.

Maintenance of your position on the E-Authentication Trusted Credential Service Providers (TCSP) list may also require periodic re-assessments. Refer to the latest version of the CAF and CAPs for details, or contact your Credential Manager.

6 Helpful Resources

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

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 Trust Credential Service Provider List contains the list of trusted Credential Service Providers 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 Initiative adopted schemes.

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

Appendix A: Acronyms and Abbreviations

Acronym	Description
CSid	Credential Service Identifier
CA	Certification Authority
CAF	Credential Assessment Framework
CAP	Credential Assessment Profile
CEWG	Credential Evaluation Working Group
COTS	Commercial off the Shelf
CRL	Certificate Revocation List
CS	Credential Service
CSP	Credential Service Provider
eGCA	eGovernance Certification Authority
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
OCSP	Online Certificate Status Protocol
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SP	Special Publication
SSL	Secure Socket Layer
TCSP	Trusted Credential Service Providers
TLS	Transport Layer Security
URL	Universal Resource Locator