



E-Authentication Handbook for Federal Government Agencies

Version 3.0.0
May 04, 2005

Executive Summary

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



Table of Contents

| | | |
|-----|--|----|
| 1 | Introduction..... | 1 |
| 1.1 | Purpose..... | 1 |
| 1.2 | Document Organization | 1 |
| 2 | E-Authentication Enabling Your Agency Application | 2 |
| 2.1 | Meet Your Agency Relationship Manager | 2 |
| 2.2 | Determine Your Agency Application’s Assurance Level..... | 2 |
| 2.3 | Execute MOA/MOU with the E-Authentication Initiative | 3 |
| 3 | Implementation..... | 4 |
| 3.1 | Assertion Acceptance Implementations | 4 |
| 3.2 | Certificate-Based Implementations..... | 8 |
| 3.3 | Agency Application Identifier | 10 |
| 3.4 | Metadata..... | 10 |
| 3.5 | Activation..... | 10 |
| 3.6 | Event Logging..... | 13 |
| 4 | Operational Responsibilities..... | 15 |
| 4.1 | Prepare Agency Help Desk to Address E-Authentication Calls | 15 |
| 4.2 | Checking and Updating Server Credentials | 15 |
| 4.3 | Federation Growth & Metadata | 15 |
| 4.4 | Server Clocks | 16 |
| 4.5 | Interoperability..... | 16 |
| 4.6 | Logos, Graphics, and Branding..... | 16 |
| 4.7 | System Availability..... | 17 |
| 5 | Maintenance, Support, and Technical Evolution..... | 18 |
| 5.1 | Modifying Your Agency Application URL..... | 18 |
| 5.2 | Technology Assessment..... | 18 |
| 5.3 | Integration Verification..... | 18 |
| 5.4 | Technology Updates | 18 |
| 5.5 | Branding Related Updates | 19 |
| 6 | Helpful Resources..... | 20 |
| 6.1 | Documents and Tools..... | 20 |
| | Appendix A: Acronyms..... | 21 |
| | Appendix B: Document History | 22 |

1 Introduction

The E-Authentication Initiative (Initiative) will simplify secure interaction with Government Agencies through a trust network that links Agency Applications (AAs) and Credential Services (CSs). The Initiative assists those who are E-Authentication-enabling AAs by providing a variety of resources, such as guidance, tools and technical information. This handbook offers guidance to Agencies regarding the Initiative, and helps you utilize Initiative resources.

This handbook provides wide coverage of topics that relate to Agencies, summarizing many of the requirements and specialized documents supporting the 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 Memorandum of Agreement (MOA). The authors of the handbook will, whenever possible, relate the subject matter under discussion to any relevant document within the body of knowledge related to the Initiative. For the entire library of E-Authentication documents, please visit <http://www.cio.gov/eauthentication/library.htm>.

1.1 Purpose

This handbook is designed to assist Agencies in E-Authentication-enabling AAs, which results in an Agency becoming a member of the E-Authentication Federation. The reader of this handbook is assumed to have a working knowledge of identity management, including SAML and Public Key Infrastructure (PKI). This handbook is written and intended for Agencies that provide online AA services to external facing end users. The ability to rely upon a definitive statement of who is interacting with an online Government AA is a cornerstone of E-Government. This handbook provides helpful guidelines for Agencies to understand the Initiative, the role of the Agency in the Initiative, steps involved in entering the community of trust, and the resources available to assist in that process. A companion Handbook for Credential Service Providers (CSPs) exists and focuses on similar information and guidelines for implementing CSs.

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

1.2 Document Organization

This handbook describes how Agencies should proceed throughout the full life cycle of Initiative participation. The document provides guidelines and recommendations based upon the following helpful categories:

- E-Authentication Enabling Your Agency Application
- Implementation
- Operational Responsibilities
- Maintenance, Support, and Technical Evolution
- Resources

2 E-Authentication Enabling Your Agency Application

Agencies are key partners in the success of the Initiative and E-Government, as Agencies make available electronic services to enable quicker, more cost effective citizen-government interaction. The 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 Initiative will designate an Agency Relationship Manager (ARM) to help your Agency navigate through the process of E-Authentication-enabling your AA. ARMs work in the E-Authentication Program Management Office (PMO) and assigned by the Program Executive (PE) to coordinate all activities related to a given AA. Your ARM will provide guidance and serve as one of your primary points of contact for the life of your relationship with the Initiative. Agencies and ARMs are encouraged to maintain close contact and working relationships with one another to ensure open channels of communication.

2.2 Determine Your Agency Application's Assurance Level

The government has outlined four levels of identity assurance per guidance from *OMB M-04-04* and NIST's Technical supplement document, *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 AA. 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 in the case of an authentication error, as 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 AA or Agency's overall mission. Furthermore, an Agency must consider any compensating controls (e.g. business processes) on a transaction basis that might lower the AA's assurance level.

The Initiative, in concert with the Software Engineering Institute (SEI) at Carnegie Mellon University, developed the Electronic Risk and Requirements Assessment (E-RA) tool to facilitate the assessment of risks associated with a false positive authentication. The E-RA tool can be downloaded from <http://www.cio.gov/eauthentication/era.htm>. Although the tool is not required, its use fulfills a requirement in the annual E-Government Act Report to OMB, required by section 202(g) of the E-Government Act, to report on AA assurance levels. Other factors, such as compensating controls, may help reduce the overall false-positive risk profile of your AA. The use of compensating controls may enable your AA 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 Initiative website (<http://www.cio.gov/eauthentication/>).

In the course of performing the AA's risk assessment, an Agency may observe that:

- Different transactions require different assurance levels
- The assurance levels of the transactions tend to be of one higher and one lower level of assurance

- Compensating controls are not available to mitigate the higher assurance level transactions
- Discrete groups (classes, types) of users tend to use exclusively either the higher or the lower assurance level transactions

Therefore, the Agency should consider segmenting¹ the AA so that only those end users who require authentication at the higher assurance level are issued those credentials.

The PMO assesses CSs to determine their level of assurance. For additional information on this assessment process refer to the CAF Suite (<http://www.cio.gov/eauthentication/CredSuite.htm>). The CS assurance level is then used within the Initiative to determine which CSs may be used to authenticate end users to specific AAs. Only CSs providing credentials, corresponding to your AA's required assurance level (or higher), are permitted to authenticate end users for access to your AA, thus ensuring that each Application's assurance level requirements are met.

2.3 Execute MOA/MOU with the E-Authentication Initiative

One of the first steps requires entering into a MOU and/or a MOA with the Initiative. The MOU/MOA covers roles, responsibilities, and any other necessary arrangements. The MOU/MOA will begin the process and formally establish an ongoing working relationship with the Initiative for your Agency. The MOU/MOA covers your commitments as an Agency, as well as the Initiative's commitment to your Agency.

¹ Segmentation may result in either two discrete AAs or one AA with multiple interfaces via different URLs.

3 Implementation

The implementation process will likely differ for each prospective AA, as it is dependent upon many factors such as assurance level, technical environment, chosen software product, and existing identity management. For assurance levels 1 and 2, AAs 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* (<http://www.cio.gov/eauthentication/documents/TechApproach.pdf>).

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

3.1 Assertion Acceptance Implementations

For AAs operating at assertion-based authentication levels, the Initiative has published a suite of technical documents related to SAML implementation. The E-Authentication Architecture 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/TechSuite.htm>.

3.1.1 Software Product Selection

The E-Authentication framework employs a Federation of CSs and AAs, and relies on no single entity to provide or guarantee credentials. The architecture is also vendor and technology neutral, which enables Agencies to select from a variety of approved software products (e.g., Commercial off the Shelf (COTS) products, toolkits, and open source software). Some software products may consist of a suite of tools. Depending upon the AA's requirements, the entire software product suite may be appropriate or may enable value-added functionality. Agencies may, under certain circumstances, develop their own "home grown" adopted scheme software product². All approved software products are published on *The Approved E-Authentication Technology Provider List* (<http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm>). Agencies should select a software product from this list to ensure the interoperability of their AA.

Despite the existence of published *E-Authentication Interface Specifications*, it is quite possible that software products will not fully comply with the *E-Authentication Interface Specifications*. To mitigate this risk, the Initiative has established the E-Authentication Interoperability Lab (Lab). The Lab's function is simple – verify the interoperability of all schemes, software products, components (e.g., Scheme Translator, Step Down Translator, Portal), AAs and CSs. Prior to Agency and CSP use, all adopted scheme software products must prove interoperability with all approved software products, and must be in compliance with the *E-Authentication Interface Specifications*.

Software product configuration recipes are available in the *E-Authentication Cookbook* (<http://www.cio.gov/eauthentication/documents/Cookbook.pdf>).

² If your Agency is interested in developing your own implementation from a toolkit or implement open source software, please be sure to advise your ARM as soon as possible. Your ARM can provide assistance regarding the policies governing the use of unapproved software.

3.1.2 Implement a Test Capability

AAs 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 Initiative to verify the operational status of an AA, and facilitates acceptance of new AAs into the operational Federation. To facilitate testing, the Initiative has defined a uniform test processing mechanism required for all AAs.

Any assertion successfully transmitted to the AA that has the Assurance Level attribute set to “Test” must result in the AA displaying a page indicating the test was successful. The *E-Authentication Interface Specifications* require the page to contain certain elements such as the common name and CS identifier (CSid). The use of a test assertion must not permit access to actual system functions. 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. This is not considered a duplicate of an AA’s full functionality; it is only a test interface to the SAML capabilities of the AA.

3.1.3 E-Governance Certificate Authority

On behalf of the E-Authentication PMO, the Federal Public Key Infrastructure Policy Authority (FPKI PA) has established the E-Governance Certificate Authority (E-GCA) whose responsibility is to issue certificates for assertion-based CSs and AAs. These certificates are for the servers of approved Federation members, not for end-user authentication. Certificates are necessary to ensure that only approved organizations can participate in the Federation.

The E-GCA has test and production environments each comprised of three Certificate Authorities (CAs), two of which are assigned to issue certificates for CSs at either assurance level one (1) or two (2). The third CA issues AA certificates. Certificates from the prototype are issued for interoperability testing (prior to approval to operate) and for operational tests of E-Authentication participants. Upon successful completion of the test, the participant is issued an approval to operate and receives the appropriate certificate(s) from the production environment.

Certificates from the E-GCA are required to secure the Simple Object Access Protocol (SOAP) channel used to pass the identity assertion between CSs and AAs. An AA must not accept assertions from a CS unless the E-GCA certificate is used to secure the SOAP channel. For an overview of the E-GCA’s role in the SAML hand-off, refer to the *SAML Artifact Profile as an Adopted Scheme for E-Authentication* document, section 4.

AAs operating at assertion-based authentication levels are required to obtain appropriate certificates from the E-GCA. To enable verification of the AA receiving the identity assertion, AAs will also need to be installed with E-GCA self-signed certificates as trust anchors. These certificates are used by the CSs to ensure they provide identity assertions to organizations that are part of the Federation. Detailed recipes for obtaining and configuring E-GCA certificates are available in the *E-Authentication Cookbook*.

3.1.4 Secure SOAP Channel

As previously described, E-GCA issued certificates are required for the Transport Layer Security (TLS)/Secure Sockets Layer (SSL) connection to secure the SOAP channel used in communicating the assertion between the CS and AA. During the TLS/SSL connection, the CS will be located on port 443 or 7676. E-GCA certificates enable both parties (CS and AA) to verify the identity of the other, and enable the transmission of the assertion without tampering, as described in the *E-Authentication Interface Specifications for the SAML Artifact Profile* document.

Table 3-1 demonstrates which E-GCA for CSs must be trusted by an AA at assertion-based authentication levels (assurance levels 1 and 2). Level 2 AAs must only trust CSs for the level 2 E-GCA, while level 1 AAs must trust both.

Table 3-1

| E-GCA | AA Assurance Level | |
|------------|--------------------|---|
| | 1 | 2 |
| Level 1 CS | √ | X |
| Level 2 CS | √ | √ |
| √ = Trust | X = Do Not Trust | |

Table 3-2 below, although similar to the previous table, describes which E-GCA issues certificates to AAs at specific assurance levels to secure the SOAP channel.

Table 3-2

| E-GCA | AA Assurance Level | |
|--------------|--------------------|---|
| | 1 | 2 |
| Level 1 CS | √ | X |
| Level 2 CS | X | √ |
| √ = Required | X = Do Not Obtain | |

AAs will also need to be installed with E-GCA self-signed certificates as trust anchors for the SOAP responder to enable verification of the AA certificates. To secure the SOAP channel, AAs will also need to present the issued E-GCA certificates during the SSL/TLS handshake.

3.1.5 Session Reset Mechanism

The SAML assertion provided by the CS contains several timestamps of interest to the AA. These timestamps include:

- IssueInstant – the time and date of when the assertion was issued
- NotBefore – the time and date of when the assertion begins to be valid
- NotOnOrAfter – the time and date of when the assertion expires
- AuthenticationInstant – the time and date of when the end user authenticated

The SAML standard specifies requirements limiting the acceptable lifetime of the assertion, but policies on how recently the end user was required to authenticate will vary between CSs³.

³ NIST SP800-63 and the CAF place some limitations on session management at the CS.

If AAs have requirements on how recently an end user authenticated, beyond what is required by the Initiative, there is a mechanism used to request the CS 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 an end user to re-authenticate, the AA 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 *Credential Assessment Framework* are deemed insufficient. Please notify your ARM if you intend to use this mechanism.

3.1.6 Testing

While the Lab tests software products for interoperability and specification compliance, the possibility of AA misconfiguration still exists. To ensure interoperability, the Lab has established processes and procedures for testing AAs. The two types of AA testing are Sandbox Testing and Acceptance Testing.

3.1.6.1 Sandbox Testing

Sandbox Testing is an informal offering of the Lab and designed to help identify misconfigurations and other issues that would prevent interoperability in accordance with the E-Authentication Interface Specifications. In preparation for testing, the Lab configures two (2) approved software products for the AA to interoperate with. If requested by the Agency, additional approved software products can be configured. During the testing of the AA, the Lab provides a supportive role for Sandbox Testing, while the Agency is responsible for executing the test procedures. If needed, the Lab is available to assist with any questions or provide additional support.

When an Agency believes the AA has successfully interoperated with the configured approved software products, the Lab will review the test logs to ensure interoperability was successful. AAs that have successfully completed Sandbox Testing are eligible to participate in Acceptance Testing.

3.1.6.2 Acceptance Testing

Acceptance Testing is required to ensure that the AA interoperates with all approved software products and is in compliance with the *E-Authentication Interface Specifications*. Before testing can begin, AAs must meet all prerequisites listed on the Testing Prerequisite Checklist. In preparation for testing, the Lab will configure the service into the SAML Server and a test Portal, ensure the E-GCA test certificate is properly configured, and prepare a test plan. For testing purposes, the AA must be configured on a system equivalent to the Agency's "production environment". Acceptance Testing is conducted by the Lab and in accordance with a developed test plan. When an AA has successfully completed Acceptance Testing, the Operations Director is notified for official approval.

Please discuss the timing and scheduling of Sandbox and Acceptance Testing with your ARM, who will request testing with the Lab.

For additional information on Sandbox and Acceptance Testing, please refer to the *E-Authentication Interoperability Lab Concept of Operations*

(<http://www.cio.gov/eauthentication/documents/LabOPS.pdf>).

3.1.7 3DES & AES

The Advanced Encryption Standard (AES) was published as a Federal Information Processing Standard (FIPS) Publication 197. FIPS 197 specifies a cryptographic algorithm (Rijndael) for use by U.S. Government organizations to protect sensitive but unclassified (SBU) information. Prior to the

approval of FIPS 197, the standard for encryption of SBU information by U.S. Government organizations was Triple Data Encryption Standard (3DES) (FIPS 46-3). Government organizations will be able to use other FIPS-approved algorithms in addition to, or in lieu of, AES. Thus, while AES was published and is being continually developed to replace 3DES, NIST anticipates that 3DES will remain an approved algorithm (for U.S. Government use) for the foreseeable future.

Unfortunately, while AES has been a published standard for several years and implementations do exist in both commercial and proprietary systems, its support in public standards is not yet complete. The original specifications for SSL and TLS predate the AES, and not all vendors have updated their software products.

Currently, the 3DES is a supported algorithm for E-Authentication, and it is likely that not all CSPs and Federal Agencies have migrated to the newer AES. Therefore, 3DES must be supported, and AES can be used if it can be negotiated in the TLS/SSL handshake. As previously mentioned, during the TLS/SSL connection, the CS will be located on port 443 or 7676.

Given the level of technological adoption and standards incorporation, full support for AES by all E-Authentication approved technology providers is uncertain and unlikely in the short term. The PMO will continually monitor NIST guidance, vendor implementations, and Federation member desire for AES support.

3.2 Certificate-Based Implementations

The following sections focus on Agencies seeking to implement certificate-based authentication for their AAs. Detailed information on 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 ARM and the 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 CAs and includes an E-Authentication trusted CA. The second level of validation ascertains the certificate's status. Both of these steps are required.

There are three main considerations in configuring an AA for certificate-based authentication; (1) determination of CS 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

Two technical options exist for your AA to determine trust at the time of end user authentication. One is to 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 a method for finding a trusted chain of certificates from your Agency's trust anchor through the FPKI to the end user's issuing CA. It is the recommended approach because it simplifies management of the AA and improves security by allowing the AA to leverage the FPKI, rather than, using a manual configuration process to replicate the security and policy information embedded in the cross-certificates.

Because processing certification paths is very complex and currently not widely supported in commercial products, the Initiative supports the Trust List approach as an interim solution. This approach relies upon a manual configuration process of keeping track of which CAs are trusted; adding new CAs to the trust list as the CAs are added to the FPKI and removing CAs that are no longer part of the FPKI. There are a number of risks to this approach. First, new trusted CAs must be manually added to the Trust List. To date, this has been an infrequent occurrence, but as Bridge-to-Bridge cross-certification continues to progress, this can become a burdensome process. Second, if trust in a

particular CA is revoked by the Federal Bridge Certificate Authority (FBCA), the AA owner must be prompt in manually removing that CA from the Trust List. Revocation of trust from the FBCA is extremely rare and would be well publicized. Finally, with this approach, the installation of trust anchors can create unconstrained trust. When the FBCA exchanges cross-certificates with approved CAs, those certificates may contain constraints that limit the types of certificates that are trusted (e.g., policy constraints or naming constraints). When using trust anchors, these constraints are not automatically applied, and an end user may be incorrectly validated. It is recommended that this approach to support certificate validation be used on a very small scale.

The Initiative maintains a list of CAs who are trusted⁴ by the E-Authentication Federation.

3.2.2 Agency Validation Service

An Agency may need to trust other CAs in addition to those trusted by the FBCA. The Initiative has designed a way for this to work seamlessly within the E-Authentication framework. 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 AA 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.

3.2.3 Certificate Status Checking

AAs that implement 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 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 configured before becoming operational. Information about how to access revocation information for each CA on the trust list is available on the Initiative website. Your AA must be configured to access revocation information for every trusted CA, including the revocation lists for E-GCA certificates.

3.2.4 Hint Lists

Certificate-based authentication for websites is accomplished by using TLS/SSL. The TLS/SSL protocol part of the handshake provides a method for 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 a trusted certificate for authentication. The list of CAs is referred to as a *hint list*.

E-Authentication enabled websites should configure the web server with an appropriate hint list in order for the AA to function properly. The list of CAs is available from the Initiative through your ARM, but the configuration of hint lists varies from product to product. For more information on the role of hint lists in the E-Authentication framework, refer to the *Technical Approach for the Authentication Service Component*, section 3.

3.2.5 End User Certificate Contents

E-Authentication end user certificates are issued by CAs that are cross-certified with the FBCA. These certificates conform to the X.509v3 Federal certificate profile. Accepting certificates for end user

⁴ The policies, procedures, and criteria used to determine assess CAs for use by E-Authentication are defined in CAF. The CAF defers assessment of CAs to the FPKI Policy Authority (FPKI PA), which controls the FBCA and E-GCA. For more information on the FPKI PA and the FBCA see <http://www.cio.gov/fpkipa/> and www.cio.gov/fbca/.

authentication requires an understanding of the fields that will be available to the AA. The data contained in the fields constitutes the minimum set of information that will be initially available to the AA. Additional information, if required, may not be available in the certificates or may be optionally available in certificates from only certain CAs.

AA owners are urged consult the *X.509 Certificate Policy for the Federal Bridge Certification Authority* for up-to-date details regarding mandatory fields in certificates issued by entities cross-certified with the FBCA. The *X.509 Certificate Policy for the Federal Bridge Certification Authority* can be found at <http://www.cio.gov/fpkipa/> along with a list of cross-certified entities.

3.3 Agency Application Identifier

Each AA is issued a unique identifier by the Initiative. This identifier, known as the AA identifier (AAid), provides all other services with a unique way of referring to your AA. If your AA 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 3.1.5 of this document. It is also used when end users are redirected to the Portal to select a CS. Please refer to the *E-Authentication Interface Specifications* for information on how and when to use the AAid in your AA.

3.4 Metadata

The Initiative publishes metadata about each participating AA and CS. This metadata is updated whenever new AAs or CSs are added to the Federation. It is recommended that AAs and CSs update their local copy of the metadata as necessary. 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*.

3.5 Activation

Activation is the process by which the end user information contained in a SAML assertion or PKI certificate is mapped by the AA to the appropriate end user in the AA's database of end users. The degree to which activation can be successfully accomplished will, in part, dictate how convenient end users perceive the AAs to be.

Activation is only required the first time an end user accesses an AA with a credential issued by a trusted member of the E-Authentication Federation. There are four basic approaches to activation: automatic, prompted, deferred, and no activation. Each will be discussed in the following sections.

3.5.1 Activation Strategies

The following sections describe the four basic approaches to activation. Agencies may choose to implement one or more of these strategies in order to maximize the success rate of activating an end user.

3.5.1.1 Automatic Activation

The AA knows the identity of the end user, per the SAML assertion or PKI certificate. Automatic activation is the mapping of the asserted identity to a specific end user in the AA's database of end users, solely from the contents of the SAML assertion or PKI certificate.

The following are the requirements for automatic activation:

- The AA must have its own database of end users that can be extended to include the CSid and User identifier (Uid) contained in the SAML assertion or the certificate issuer and serial number contained in the PKI certificate

- There must be a high degree of confidence that the information in the database of end users is accurate and current
- The AA's activation process must employ policies and/or techniques that are capable of correctly matching the identity of the end user in the AA's database of end users, using only the attributes presented in the SAML assertion or PKI certificate
- Automatic activation should be attainable a high percentage of the time⁵

Example: Agency "A" has added code to their AA to collect the attributes contained in the SAML assertion (specifically, the optional attributes including partial Social Security Number (SSN), full name, and date of birth) and match that information against the corresponding information in their local user store. The Agency's expectation is that they will be able to successfully activate an end user a high percentage of the time. End users that cannot be successfully activated using this approach could be activated using either prompted activation or deferred activation.

3.5.1.2 Prompted Activation

Prompted activation is the mapping of the asserted identity to a specific end user in the AA's database of end users, from the contents of the SAML assertion or PKI certificate, and/or additional information obtained by the AA prompting the end user.

The following are the requirements for prompted activation:

- The AA must have its own database of end users that can be extended to include the CSid and Uid contained in the SAML assertion or the certificate issuer and serial number contained in the PKI certificate
- There must be a high degree of confidence that the information in the database of end users is accurate and current
- The Applicant's activation process must employ policies and/or techniques that are capable of correctly matching the identity of the end user in the database of users using the attributes presented in the SAML assertion or PKI certificate, which is in conjunction with additional information obtained by the AA prompting the end user
- Alternatively, the AA may employ an external knowledge-based service provider to assist in the activation process
- Prompted activation should be attainable a high percentage of the time⁶

Example: Agency "B" has determined that the attributes in the SAML assertion are not sufficient to uniquely identify an end user. The AA will prompt the end user to provide some piece of shared special knowledge, which will then allow the AA to correctly map to an end user in the AA's database of end users.

Prompted activation could be used either alone or in addition to automatic activation, but only if automatic activation was unable to map an identity assertion to the AA's database of end users.

3.5.1.3 Deferred Activation

Deferred activation is an out of band process which is used to map the end user represented by the SAML assertion or PKI certificate and the end user stored within the AA's end user database. The out of band process typically will not occur in real time.

The following are the requirements of deferred activation:

⁵ An AA pilot project has shown activation rates in the 89% - 96% range using automatic activation.

⁶ An AA pilot project has shown activation rates in the 89% - 96% range using prompted activation.

- The AA must have its own end user database that can be extended to include the CSid and Uid contained in the SAML assertion, or the certificate issuer and serial number contained in the PKI certificate
- The AA does not have suitable matching policies and/or techniques available
- The Agency itself has a suitable mechanism for contacting the end user to confirm the end user's identity
- The AA may optionally allow the end user certain limited rights or access pending satisfactory completion of the activation process

Example: Agency "C" has E-Authentication enabled an AA. Before an end user is actually allowed to access the AA, the end user must be approved by an official from the end user's organization who has been previously designated as an "approving authority." The AA uses a secondary process that allows the end user's organization designee to authorize access for the end user.

3.5.1.4 No Activation

No activation is defined as an AA that either has no user database to map the information contained in the SAML assertion or PKI certificate to, or the end user is unknown to the AA. The nature of the AA is such that the end user may be allowed immediate access to the AA following completion of a new end user registration process.

Example: Agency "D" has an AA such that past interaction/transaction processing with the AA is not a prerequisite for future interaction with the AA. Thus it is not necessary for the AA to uniquely identify an end user against the AA end user database. Instead, the AA will create a new end user entry in the end user database whenever a new end user authenticates to the AA.

3.5.2 Activation Strategy Selection

SAML assertions and PKI certificates may contain optional attributes. The use of optional attributes may optimize automatic activation by providing additional information to resolve more common names, such as multiple John Smiths. AA owners are advised to verify what attributes are provided in the SAML assertions or PKI certificates from various CSs as part of determining their activation strategy selection.

3.5.3 Support for Multiple Credentials

A federated identity system allows an end user to access an AA using any trusted credential having the appropriate assurance level. By allowing end users to employ one credential for use at many AAs, a business objective of reducing the required set of credentials to access government AAs is achieved.

Activation will, in most cases, be a "one time" event for any given end user; however, AAs must support the end user who was previously activated with one credential service and then wishes to access the AAs at some later date with a different CS.

The following are possible alternatives that an Agency may wish to consider for supporting this scenario. Each approach has its own unique advantages and disadvantages. An Agency must determine which approach will provide its end users with the most satisfactory experience.

3.5.3.1 Support 2 or More Different Credentials

The Agency may choose to map the various credentials to the same end user within the AA's end user database.

3.5.3.2 Support Via Overwrite

The Agency may choose to support activation with a second credential by overwriting the end user database entry created by activation performed using the initial credential. If an Agency chooses this approach, end users should be notified so that they understand the potential impact.

3.5.3.3 Create a New User in the Local Store

The Agency may choose to create a new entry in the AA's end user database. The AA then has the option of linking the various credentials activated to a single end user or may consider the end user to be different for each credential used. If an Agency chooses this approach, end users should be notified so that they understand the potential impact.

3.5.4 Activation Failure

3.5.4.1 Hybrid Activation Strategies

In the event an AA employs automatic activation and an activation attempt fails (i.e., the AA is unable to uniquely match the end user in the local end user store to the end user represented by the SAML assertion or PKI certificate), the AA may then wish to use the prompted activation approach or the deferred activation approach.

3.5.4.2 Use of a "Landing Page"

In conjunction with a failed activation attempt, using either automatic or prompted activation, an AA should send the user to a "landing page"⁷ where the end user is provided with an explanation of the failed activation and information on how to contact the appropriate Help Desk.

Direction of an end user to a landing page is also appropriate for an AA that is using differed activation.

3.6 Event Logging

Event and audit logging is an important part of AA operations and maintenance, and enables critical capabilities, including forensics, debugging, and even business intelligence. These capabilities require that AAs store enough information so that transactions can be uniquely reconstructed at a later date.

One approach to ensuring comprehensive event logging throughout a transaction is to evaluate the interfaces between all components (e.g., Firewall, SAML Receiver, Enterprise Session Context) of an AA. To enable post-transaction analysis, each interface point should be reviewed to ensure the proper information is logged between all components. Such analysis should be done on a routine basis as a part of internal procedures that will ensure compliance with current data storage regulations.

⁷ A "landing page" is a URL where a user may be directed based on specific criteria, such as certain error conditions or the user has completed processing and needs to be brought to a page where the E-Authentication can assist the end user in determining what action to take next.

The E-Authentication PMO has developed a chart (Table 3-3) to assist Agencies in understanding the lifecycle of a transaction. The chart is generic and is intended to be adapted to your particular AA architecture. Use of this chart is optional, but may help clarify needs or opportunities for logging capabilities.

Table 3-3

| | Events | Logging | | | | | |
|---|--|---------|----|----------|---------------|----|----------------------------|
| | | Portal | CS | AA | | | |
| | | | | Firewall | SAML Receiver | AA | Enterprise Session Context |
| 1 | The end user starts at the Portal and selects the AA. They then select a CS to access the AA. | √ | | | | | |
| 2 | The Portal redirects the end user to the CS website to authenticate. | √ | √ | | | | |
| 3 | Once authenticated, the CS creates an artifact and assertion for the end user, and redirects the end user to the AA's SAML receiver. | | √ | √ | √ | | |
| 4 | The AA returns the artifact to the CS, and receives an assertion identifying the end user. | | | | √ | | |
| 5 | The end user is registered with the enterprise-wide session context and passed to the AA to continue the transaction. | | | | | √ | √ |

4 Operational Responsibilities

This section provides guidance on operational requirements related to the Initiative. E-Authentication technical specifications describe these requirements, and 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 Initiative.

4.1 Prepare Agency Help Desk to Address E-Authentication Calls

There may be instances in which an end user contacts your AA help desk or technical support to report an issue.

Your help desk is not required to answer specific questions regarding the Portal or specific CSs. However, your staff must be familiar with your AA within the context of the E-Authentication system, and be capable of escalating general issues to the E-Authentication call center/help desk. The E-Authentication call center/help desk will then escalate the issue to the appropriate personnel. Your help desk should also be aware of any bulletins or announcements from the PMO (e.g. announcements of downtime at a particular CS) and be prepared to respond accordingly.

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 AA or one of the trusted CSs. Knowledge of the Portal, and which CSs are applicable is also recommended, as is awareness of any special relationships with CS(s).

4.2 Checking and Updating Server Credentials

To ensure smooth, continual operation of the E-Authentication system, the Initiative requires that all participants maintain valid server certificates from the E-GCA⁸. This requirement is outlined in section 2 of the *SAML Artifact Profile as an Adopted Scheme for E-Authentication*. If certificates are approaching their expiration date, please be sure to contact your ARM to coordinate the issuance of a new certificate. If certificates are compromised or expired, please alert your ARM immediately.

The *E-Authentication Interface Specifications* require your AA to detect attempted SAML hand-offs without appropriate credentials. Please report these and any other security related events to the E-Authentication call center/help desk as soon as possible.

4.3 Federation Growth & Metadata

As a critical foundation element to E-Government, the Initiative is open to all Agencies and actively pursues partnerships with industry and potential CSPs. These efforts will result in an ever-growing Federation of CSs and AAs, which may provide your end user base with additional credentials that will work with your AA. To manage and coordinate the Federation, metadata is published to participants. The metadata provides important attributes such as assurance level and website Universal Resource Locator (URL). An initial set of metadata will be used to configure your AA during implementation, but the metadata is updated continuously. AAs and CSs 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-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*.

⁸ For assertion-based authentication levels.

4.4 Server Clocks

Accurate timekeeping within the Federation is critical. Assertion-based authentication typically carries with it a timestamp indicating when it was created, and a second indicating the duration during which the CS 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.

Whether receiving or making an assertion, keeping accurate time is important. If the server clock is incorrect, a CS may generate assertions that seem to come from the future, or are already expired. An AA may interpret assertions similarly. If you have set identity refresh policies for your AA that require updated authentication prior to interacting with end users, this policy may manifest itself incorrectly based upon an incorrect server clocks.

To ensure proper compliance of these policies, your Agency must 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. Other commonly accepted time sync methods include Global Positioning System (GPS) and the NIST Automated Computer Time Service (ACTS).

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 Initiative aggressively tests to ensure interoperability, there is the possibility that end user access may be impaired due to misconfiguration or improper implementation of an AA. In order to minimize the impact of such an event on the greater Federation, the Portal has the capability to disable specific CS-AA pairs during problem periods. This enables the Initiative, in conjunction with the CSP and Agency, to audit/troubleshoot the interoperability issue(s), and restore interoperability promptly. The E-Authentication framework inherently supports this capability, requiring no changes on the part of any CSP and/or Agency. To facilitate such troubleshooting, the PMO may request, from time to time, AA 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 ARM anytime the problems arise so that the Portal can be updated and the resolution process can begin.

4.6 Logos, Graphics, and Branding

As a member of the E-Authentication Federation, your Agency will be allowed to display a small E-Authentication logo on your AA 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 AA website elsewhere in the E-Authentication system (e.g., Portal, CS). These graphics, images, or text will help establish consistent branding and messaging throughout the E-Authentication system, so that end users can easily identify your AA. Your MOU/MOA may also provision these images for use in other materials and forums.

4.7 System Availability

System availability awareness is critical, especially when systems rely upon one another. The PMO recognizes this and the impact of availability on the reputation and serviceability of the E-Authentication Federation. To facilitate awareness and mitigate the effects of system downtime, the E-Authentication Enterprise Operations Center (EOC) has adopted two parallel approaches.

The PMO will establish a proactive awareness mechanism to escalate unexpected unavailability situations. To do so, the EOC will need to monitor production Federation services remotely on an ongoing basis. In addition, all Federation members are required to proactively communicate planned system unavailability (e.g., maintenance, upgrades, etc) as soon as possible. The ARM and the EOC Client Services team will coordinate the appropriate actions within the Federation, such as CS or AA deactivation and Help Desk notices. In doing so, the EOC may request additional or supplementary information concerning the status of the system or the planned restoration of services.

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 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 Agency Application URL

Please be sure to notify the E-Authentication call center/help desk in advance if the URL for your AA is going to be changed. Upon notification, the E-Authentication call center/help desk will take the appropriate actions to update the URL in the E-Authentication metadata. The metadata is provided to all Initiative participants. Updating your URL in the metadata will enable CSs to continue providing credentials for your AA. The Portal will also be updated with 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 extend the technology refresh cycle. Most private industry and Agency portfolio management processes include a technology assessment for refreshment consideration. E-Authentication components should be provided in your portfolio review process, but as a relatively new Initiative, these components may require a higher-frequency refresh cycle for the short term.

5.3 Integration Verification

Prior to the deployment of an AA, the Initiative recommends that you conduct internal interoperability and functional verification tests with any implemented software products or versions related to the Initiative. Although the Lab verifies interoperability with approved software products, 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 AA will continue to interoperate.

New AAs added to your infrastructure must also be issued an AAid and tested by the Lab for interoperability and compliance with the *E-Authentication Interface Specifications*.

5.4 Technology Updates

Each Agency must ensure that any technology updates or environment changes comply with Initiative requirements. Interoperability approval of adopted scheme software products is version specific. Agencies should use approved versions in production environments associated with the Initiative. The Initiative does not perform functionality or performance testing. Therefore, prior to acquiring an adopted scheme software product, Agencies should fully inspect, review, and ensure the selected software product supports Agency requirements. Furthermore, be sure the Initiative has approved the version of your chosen software product before installation.

Prior to updating your AA in a manner that could affect E-Authentication (e.g., software product), please remember to notify your ARM. Your ARM will need to assess the situation and, if necessary, schedule an acceptance test with the Lab. Re-testing for interoperability is required to ensure that all Initiative participants have implemented and configured their systems correctly. ARMs try to stay familiar with the activities of their assigned Agencies to ensure they provide the best possible service.

Informal notification to your ARM 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 AA is provided at the Portal. The Initiative urges all Agencies to communicate any branding changes to their assigned ARM 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 AA.

6.1 Documents and Tools

- The Initiative maintains a website to provide easy access to E-Authenticated related information. The website also hosts a repository of documents related to the 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>
- The Electronic Risk and Requirements Assessment (E-RA) provides Agencies with a guide to assist in selecting the appropriate level of authentication for their AA.
Available at <http://www.cio.gov/eauthentication/documents/eraguide.pdf>
- The Trusted Credential Service Provider 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/TechSuite.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>
- The E-Authentication Cookbook provides detailed descriptions of technical and non-technical procedures, including software and hardware configuration guides.
Available at: <http://www.cio.gov/eauthentication/documents/Cookbook.pdf>

Appendix A: Acronyms

| Acronym | Description |
|----------------|--|
| 3DES | Triple Data Encryption Standard |
| AA | Agency Application |
| AAid | AA Identifier |
| ACTS | Automated Computer Time Service |
| AES | Advanced Encryption Standard |
| AVS | Agency Validation Services |
| CA | Certification Authority |
| CAF | Credential Assessment Framework |
| COTS | Commercial off the Shelf |
| CRL | Certificate Revocation List |
| CS | Credential Service |
| CSid | Credential Service Identifier |
| CSP | Credential Service Provider |
| E-GCA | E-Governance Certificate Authority |
| EOC | Enterprise Operations Center |
| E-RA | E-Authentication Risk and Requirements Analysis |
| FBCA | Federal Bridge Certification Authority |
| FPKI | Federal Public Key Infrastructure |
| FPKI PA | Federal Public Key Infrastructure Policy Authority |
| GPS | Global Positioning System |
| 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 |
| PE | Program Executive |
| PKI | Public Key Infrastructure |
| PMO | Program Management Office |
| SAML | Security Assertion Markup Language |
| SEI | Software Engineering Institute |
| SOAP | Simple Object Access Protocol |
| SP | Special Publication |
| SSL | Secure Sockets Layer |
| SSN | Social Security Number |
| TLS | Transport Layer Security |
| Uid | User Identifier |
| URL | Universal Resource Locator |

Appendix B: Document History

| Status | Release | Date | Comment | Audience |
|----------|---------|----------|---|----------|
| Release | 1.0.0 | 07/30/04 | Official release of document. | Public |
| Revision | 1.0.1 | 04/05/05 | <ul style="list-style-type: none"> ▪ Re-titled section 3.1.1 to Software Product Selection and specified that federation members can select from a variety of software products (CR #5). ▪ Specified that the use of a test assertion must not permit access to system functions (section 3.1.2) (CR #6). ▪ Provided additional information on the E-GCA (section 3.1.2) (CR #7). ▪ Added Acceptance and Sandbox Testing section under Implementation (section 3) (CR #2 & 3). ▪ Added 3DES & AES section under Implementation (section 3) (CR #8). ▪ Added End User Certificate Contents section under Implementation (section 3) (CR #9). ▪ Added Event Logging section for Implementation, which included the addition of the PMO transaction lifecycle chart. (section 3) (CR #10). ▪ Added Activation section under Implementation (section 3) (CR #1). ▪ Specified the importance of accurate timekeeping for server clocks (section 4.4) (CR #4). ▪ Added System Availability section for Operational Responsibilities (section 4) (CR #11). ▪ Replaced COTS products with software products (section 3.1.1) (CR #5). ▪ Removed test CA from tables 3-1 and 3-2 (section 3.1.4) (CR #12). ▪ Removed the reference of recipes that are not provided in the Cookbook throughout the document (CR #13). ▪ Add reference to the adopted scheme document for additional information on metadata (section 3.5) (CR #14). ▪ Replaced Credential Service with CS (except during first use) throughout the document (CR #15) ▪ Placed all document references in italic font (CR #16). ▪ Replaced E-Authentication Initiative with just Initiative (except during first use) throughout the document (CR #17). ▪ Replaced user with end user throughout the document (CR #18). ▪ Removed abbreviations from the title of | Limited |

| | | | | |
|----------|-------|----------|--|---------|
| | | | Appendix A (CR #19). | |
| | | | <ul style="list-style-type: none"> ▪ Removed third paragraph of section 3.2 (CR #20). ▪ Replaced E-Authentication architecture with E-Authentication framework throughout the document (CR #21). ▪ Move first paragraph of section 3.1 to section 3 (CR #22). ▪ Changed E-Authentication Risk and Requirements Assessment to Electronic Risk and Requirements Assessment (CR #23). | |
| Revision | 1.1.0 | 04/06/05 | Released to the PMO for update approval. | PMO |
| Revision | 1.1.1 | 04/08/05 | <ul style="list-style-type: none"> ▪ Section 1.1, line 1. Changed “results an” to “results in an” (CR #24). ▪ Section 2, line 3. Changed “are government employees working in” to “work in” (CR #25). ▪ Section 2.2, line 1. Changed “OMB M-04-04 and its technical supplement document, NIST SP 800-63” to “OMB M-04-04 and NIST’s Technical supplement document, SP 800-63” (CR #26). ▪ Section 3.1.1, 2nd paragraph, line 8. Changed “product” to “products” (CR #27). ▪ Section 3.1.3. Changed repeated use of “E-GCA CA” to “E-GCA” (CR #28). ▪ Section 3.1.3, line 6. Changed “The third SA is issues” to “The third issues” (CR #29). ▪ Section 3.2.1. Replaced section paragraphs with text provided by Steve Sill (CR #30). ▪ Removed section 3.4 (Logos, Graphics, and Branding) as is a duplicate of section 4.6 (CR #31). ▪ Section 3.6.1.1. Corrected footnote 5 font, and changed footnote text from “prompted activation” to “automatic activation” (CR #32). ▪ Section 3.6.1.2. Corrected footnote 6 font (CR #33). ▪ Section 2.6.4.2. Corrected footnote 7 font (CR #34). ▪ Section 4.6. Changed “As discussed in section 3.4” to “As a member of the E-Authentication Federation” (CR #35). ▪ Changed “federation” to “Federation” throughout the document (CR #36). ▪ Section 3.1.1. Moved last sentence of second paragraph to last sentence in first paragraph (CR #37). ▪ Section 3.1.4. Added SSL/TLS connection port requirements (CR #38). ▪ Section 3.1.7. Added SSL/TLS connection port requirements (CR #39). ▪ Section 4.1, line 5. Replaced “Agency Relationship Manager” with E-Authentication call center/help desk. Also added sentence | Limited |

| | | | | |
|----------|-------|----------|---|---------|
| | | | <p>explaining that the help desk will escalate the issue (CR #40).</p> <ul style="list-style-type: none"> ▪ Section 4.2, line 9. Replaced “Agency Relationship Manager” with E-Authentication call center/help desk (CR #41). ▪ Section 4.2, line 10. Replaced “Portal” with “AA or CS” (CR #42). ▪ Section 4.7, line 10. Replaced “Agency Relationship Manager” with E-Authentication call center/help desk (CR #43). ▪ Section 5.1, line 1 & 2. Replaced “Agency Relationship Manager” with E-Authentication call center/help desk (CR #44). ▪ Section 5.3. Added text describing that the Application must be provided an AAid along with being tested (CR #45). ▪ Section 5.4. Provided statement specifying that E-Authentication does not perform functionality or performance testing (CR #46). ▪ Section 5.4. Replaced “Agency Relationship Manager” with E-Authentication call center/help desk (CR #47). | |
| Approved | 2.0.0 | 04/11/05 | Approved by the PMO. | Public |
| Revision | 2.0.1 | 04/21/05 | <ul style="list-style-type: none"> ▪ Section 3.1.3. Added new E-GCA information provided by Cheryl Jenkins & Dave Simonetti (CR #50). ▪ Section 3.1.4. Replaced CA with CS in section text and in tables 3-1 and 3-2 (CR #51). ▪ Section 3.2.1. Replaced section paragraphs with text provided by Cheryl Jenkins & Dave Simonetti (CR #52). ▪ Section 3.1.6. Added reference to Conops (CR #48). ▪ Section 3.1.6.2. Change notification of PMO to notification of Operations Director (CR #49) | Limited |
| Revision | 2.0.2 | 05/03/05 | <ul style="list-style-type: none"> ▪ Section 3.2.3, 1st paragraph. Replaced “requires” with “provides a method for” (CR #54). ▪ Section 3.2.3, 2nd paragraph. Replaced “must” with “should” (CR #55). ▪ Moved section 3.2.5 (Agency Validation Service) to after 3.2.1 (Determination of Trust) (CR #56). ▪ Changed “Application” to “AA” throughout the document (CR #57). ▪ Added Agency Relationship Manager (ARM) acronym and use throughout document (CR #58). ▪ Section 2.3. Added a sentence describing the consideration of compensating controls (CR #59). ▪ Section 3.5.3.2. Added a sentence describing that end users should be notified when an | Limited |

- activation method is chosen (CR #61).
- Section 3.1.4, 2nd paragraph. Replaced “should” with “must” (CR #62).
- Section 3.4. Added “added to the federation” to the end of the 2nd sentence (CR #63).
- Section 3.6. Replaced “lay out” with “in understanding” (CR #64).
- Section 1. Replaced “corpus of documents” with “body of knowledge” (CR #65).
- Section 3.1.1. Replaced “be a product suite” with “consists of a suite of tools” (CR #66).
- Section 3.1.1. Added link to the E-Authentication Cookbook (CR #67).
- Section 1.1. Added sentence stating the reader is assumed to be familiar with identity management, including SAML and PKI (CR #68).
- Section 2.2. Added text describing segmenting the AA (CR #69).
- Section 2.2. Specified that the risk assessment considers impacts based on an authentication error (CR #70).
- Section 3.1.1, 1st sentence. Replaced “uses” with “employs” (CR #71).
- Section 3.1.6.2. Added sentence specifying that an AA must be configured on a system equivalent to the Agencies “production environment” (CR #72).
- Section 3.4. Replaced “on a periodic basis” with “as necessary” (CR #73).
- Section 3.1.5. Added the additional timestamps provided in the SAML assertion (CR #74).

| | | | | |
|----------|-------|----------|--|--------|
| Revision | 2.1.0 | 05/03/05 | Released to the PMO for update approval. | PMO |
| Approved | 3.0.0 | 05/04/05 | Approved by the PMO. | Public |