E-Authentication
Credential Assessment Framework
(CAF)

Business Owner: Federation Management
Creation Date:
Last Updated: 03/16/05
Version: EA-DD-0033-2.0-F
Audience: Public

Release Notes

PMO Approved

Executive Summary

This document describes the framework used by the E-Authentication Program Manager's Office (PMO) to assess Credential Service Providers (CSP) and their Credential Services (CS) for use by the E-Authentication Initiative. Governance, approach, and processes are described. The specific criteria used in the assessment process are not covered in this document; they are expressed in Credential Assessment Profiles (CAPs) described in Section 4.

This document may be used by CSPs whose services are being assessed, and by relying parties who require assurance as to the veracity of identity credentials. In addition, this document alerts these organizations as to the qualifications of Assessors, how they should expect an Assessor to perform assessments, how to interpret criteria, and make professional judgments regarding evidence.

It is expected that as the CAF is used and the number of Assessments undertaken increases, this document will evolve and be extended to reflect the experience gained from conducting actual assessments.

The E-Authentication Initiative maintains a Trust List, which contains the CSs that can be used by the Initiative. CSPs go through an application process before they are assessed. The assessment process is governed by Credential Assessment Profiles, which establish the requirements for CSs at the four Assurance Levels. The assessment produces a recommended Assurance Level to the E-Authentication PMO, which makes the final decisions on additions to the Trust List.

Document History

See Appendix D for a detailed listing.

Editors

Chris Louden	Judy Spencer	Bill Burr
Kevin Hawkins	David Temoshok	John Cornell
Richard G. Wilsher	Steve Timchak	Stephen Sill
Dave Silver	Von Harrison	

Table of Contents

Figures

1 INTRODUCTION

This document describes the processes involved in making individual identity credentials available to the E-Authentication Initiative (Initiative). This is a normative specification. Processes described herein are mandatory, except for those sections that explicitly grant latitude or subjective judgment.

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

The scope of the Initiative is remote electronic authentication of human users to Federal agency IT systems over a network. It does not address the authentication of a person who is physically present.

Critical to the success of the E-Authentication project is the assessment and approval of Credential Service Providers (CSPs). The Credential Assessment Framework (CAF), based on technical and policy guidance from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST), provides a structured means of delivering assurances to Federal agencies as to the veracity, and thus dependability of identity credentials and tokens. This assurance is achieved by evaluating and assessing CSPs and their credential-issuing service(s), in a consistent, complete, and professional manner, against criteria established in the CAF Suite.

The processes discussed in this document are based on best practices drawn from the security and audit industries as well as relevant principles and standards adopted from the General Accounting Office's Government Auditing Standards: July 1999, commonly referred to as the 'Yellow Book'.

1.1 Special Terms

This document relies on terminology defined in NIST Special Publication 800-63, version 1.0.1 '*Recommendations for Electronic Authentication*', and the OMB '*Guidance for E-Authentication*'. See Appendix B, Glossary, for a complete listing of terms used in this context.

1.2 Related Documents

The OMB E-Authentication Guidance (OMB M-04-04), and NIST Special Publication 800-63 version 1.0.1 documents establish the E-Authentication Assurance Levels and their technical requirements.

OMB M-04-04 defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria for determining the level of E-Authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction. This document is available at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

NIST Special Publication 800-63 provides technical guidance to Federal agencies implementing electronic authentication. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions. This document is available at http://csrc.nist.gov/publications/nistpubs/

These documents may be considered prerequisite reading for this document; it is assumed the reader is familiar with the concepts they establish.

The specific criteria used to assess Credential Services (CSs) are grouped into Credential Assessment Profiles (CAPs), which are described in Section 4.

Authentication Service Component (ASC) Interface Specifications describe the requirements for CSPs to technically interoperate with the Initiative. The most recent version of these documents can be found at http://www.cio.gov/eauthentication/.

The CAF, Password CAP, Certificate CAP, and Entropy Spreadsheet currently comprise the CAF Suite, which governs the Initiative. The CAF Suite listing is maintained on the E-Authentication website, and is available at (http://www.cio.gov/eauthentication/CredSuite).

1.3 General Approach

The Initiative has tremendous value to Government. It saves money by reducing redundant functions across agencies, and establishes common and consistent approaches to E-Government identity management. The services offered by the Initiative are relied on across Government, and so its management must be deliberate, diligent, consistent, and open. This section provides a general overview of the approach the Initiative takes toward the assessment and use of CSs.

The Initiative maintains a list of Trusted Credential Services that have been evaluated for use by the Federal Government. Each of these CSs is assessed to a particular Assurance Level as defined by the OMB and NIST Guidance documents. The list of assessed CSs that have been approved and their associated Assurance Levels comprise the Trusted Credential Services List ("The Trust List"). Any application participating in the Initiative can make use of any CS on the Trust List, so long as the assessed Assurance Level meets or exceeds the Assurance Level of the application.

The first step for a CS to be added to the Trust List is for the CSP to apply for an Assessment. If it is determined to be in the best interest of the Government, the CS will be assessed to determine its Assurance Level. The Assessment is performed against specific criteria that are defined in the applicable CAP. The CSP must submit evidence that shows compliance for each of the criteria elements in the applicable CAP. The evidence is then validated by an Assessment Team, which is designated by the E-Authentication Program Manager (PM).

When the assessment is complete, the PM reviews the results and makes the final determination as to whether the CS will be added to the Trust List. For those CSPs that meet the criteria, the PMO issues *Approval to Operate* to the CSP, at the determined Assurance Level, in the form of an entry on the Trust List, and a formal approval of the written Assessment Report.

A Credential Manager is assigned by the PM to manage the Assessment process. The Credential Manager also has an ongoing maintenance responsibility to ensure the CS remains compliant over time.

As technologies change or new technology is made available, additional CAPs may be developed by the Initiative. The PMO must approve each CAP before it becomes effective. See Appendix A for an overview diagram of the overall CAF Suite change and approval process.

2 GOVERNANCE

2.1 Governing Organizational Structure

The Initiative is governed by the Executive Steering Committee (ESC), which is comprised of executives from each of the agencies involved in the Initiative. The General Services Administration (GSA) is the managing partner for the Initiative, and the PMO is run by GSA Federal Technology Service (FTS). Additional information is available at http://www.cio.gov/eauthentication/.

The Federal Public Key Infrastructure Policy Authority (FPKI PA), under the auspices of the Federal Identity and Credentialing Committee (FICC), governs assessment of CSs with Public Key Infrastructure (PKI) credentials. The Initiative uses PKI certificates, but defers their governance to the FPKI PA. The E-Authentication Assurance Levels for PKI certificate-based CSs are based on policy mapping determinations made by the FPKI PA. A full description of FPKI governance is beyond the scope of this document, and additional information is available at http://www.cio.gov/fpkisc/. The Certificate CAP describes specific mapping for certificate-based CSs to E-Authentication Assurance Levels.

2.2 Roles and Responsibilities

The following sections provide the roles and responsibilities involved in governance of Initiative CSs.

2.2.1 Executive Steering Committee (ESC)

The ESC is an intergovernmental committee comprised of executives from each agency participating in the Initiative.

The ESC represents the relying parties for the Initiative and advises the PMO, but is not involved in the day-to-day activities. The ESC provides funding to the Initiative, and receives status updates from the PMO.

2.2.2 Program Management Office (PMO)

The PMO is the organization within GSA-FTS that handles program management, administration, and operations for the Initiative. All contracts, licensing, and participation agreements related to the Initiative are executed and managed by the PMO. In addition, the PMO reviews and approves the CAF suite of documents.

2.2.3 Program Manager (PM)

The PM is the executive in charge of the PMO. In addition to the daily management of the PMO, the PM has the following responsibilities:

1. Approval of Assessment Recommendation. The PM has the final authority on any matters related to the Trust List, including whether to accept the recommendations of assessments.
2. Assigning Credential Managers. Each CS has an assigned Credential Manager from the PMO. Responsibilities of the Credential Manager are described below.
3. Assigning Unique Case Numbers. The PM assigns a unique case number to each Application for Assessment.
4. Designation of Assessors. The PM determines who is approved to perform assessments for the Initiative, based on qualification criteria. In addition. The PM maintains a list of active and approved Assessors.
5. Designation of Credential Evaluation Working Group (CEWG) Members. The PM will select candidates for the CEWG based on nominations from the ESC or other sources for qualified volunteers. See Section 2.2.7 for details regarding the CEWG.
6. Determine Assessment Schedule. The PM determines the assessment schedule, in accordance with Initiative priorities and the best interests of the Government.
7. Determine Need for Re-assessment. The PM determines whether CS changes are sufficient to require re-assessment. In addition, the PM initiates re-assessments if the PM determines that updates to any CAP may affect the Assurance Level of CSs.
8. Override Decision to Reject Application. The PM can, upon review, override the CEWG's decision to reject an application.

The PM may delegate any of these responsibilities as needed.

2.2.4 Credential Manager

A Credential Manager is a Government employee working in the PMO. They are assigned by the PM to manage all activities related to a given CS. A Credential Manager may be responsible for several CSs and may have other responsibilities within the PMO. The Credential Manager's responsibilities are:

1. Applicant CSP Management. The Credential Manager is assigned as soon as an Application for Assessment is received. The Credential Manager is responsible for managing and coordinating the application process described in Figure 1. They will present a summary of the CS to the CEWG.
2. CS Assessment. The Credential Manager coordinates and manages the credential assessment, participates in the preparation of the Assessment Report, and presents the recommendation to the PM.

3. Notify PM of Assessment Termination. Upon receipt of written notification from the Assessment Team that an Assessment has been terminated prior to completion, the Credential Manager will notify the PM.
4. CS Maintenance. Every CS on the Trust List has a Credential Manager assigned to ensure appropriate credential maintenance responsibilities are met.
5. Determine Applicable CAP. The Credential Manager determines which CAP is applicable and notifies the CSP.

2.2.5 Assessment Team

The Assessment Team is comprised of Assessors designated by the PM to evaluate a CSP against the applicable CAP. Additional information on Assessments is available in Section 3.2. Assessors may be contractors, but cannot be affiliated with the CS being assessed. Every Assessment produces a written Assessment Report and a Recommendation. The Recommendation specifies whether the Assessment Team believes the CS should be included on the Trust List, and if so, at which Assurance Level.

The Assessment Team and individual Assessors should be organizationally independent from the CSP whose service(s) they are assessing. Assessors should maintain independence so that judgments and recommendations will be impartial. If any circumstance affects an Assessor's ability to perform the Assessment and to report findings impartially, that Assessor should decline to perform the Assessment. The Assessment Team may be required to sign Non-Disclosure Agreements with the CSP or declare any potential conflicts of interests relating to an assessment.

2.2.5.1 Assessor Qualifications

The selected Assessment Team shall collectively possess adequate technical proficiency and industry knowledge for the specific Assessment being performed. Established qualifications for Assessors must enable competent determination of Credential Services' compliance to applicable CAP criteria, taking into account technical issues, the Assurance Level being sought, and specific requirements that the criteria might set out (e.g., specific management systems). The Assessment Team shall have, as a minimum:

- Thorough knowledge of the government's E-Authentication requirements;
- Understanding of the CSP's industry;
- Expertise in the specific technologies/techniques being assessed;
- Technical and management audit appreciation;
- Familiarity with the CAF Suite and its principles of operation.

In addition, all Assessments shall be the responsibility of a Lead Assessor who shall have the following specific audit capabilities:

- **At Assurance Level 1** - No additional stipulation
  - *Equivalent criterion* - CSPs may make a self-declaration of their information security practices or provide evidence of a SAS-70 audit (or equivalent).
- **At Assurance Level 2** - As a minimum, have been performing as an independent auditor in the field of information security at least four times over the preceding 12 month period.
  - *Equivalent criterion* - CSPs must be audited by an independent auditor at least every 24 months to ensure the organization's information security-related practices are consistent with the policies and procedures for the specified service and the appointed auditor must have appropriate accreditation or other acceptable experience and qualification.
- **At Assurance Levels 2-4** – Certificate-based Credential Services approved by the FPKI Architecture will be granted approval automatically.

2.2.6 Credential Service Provider (CSP)

The CSP is the organization that offers a particular CS. The CSP may be a public or private entity, but it must have the authority to make binding commitments regarding the CS. In addition to establishing and operating a CS, the CSP has the following responsibilities:

1. Application for Assessment. If a CSP is interested in offering a CS for use in the Initiative, they must prepare and submit the Application for Assessment. (See Section 3.1)
2. Assessment Package. If the CEWG accepts the Application for Assessment, the CSP must prepare and submit an Assessment Package, which includes evidence of compliance with the applicable CAP. (See Section 3.2.1)
3. CS Assessment. When the assessment begins, the CSP must submit itself to an audit of any element of the Assessment Package that has not been independently audited by a recognized auditor. See Section 3.2 for more information.
4. CS Maintenance. Once a CS becomes part of the Trust List, certain maintenance activities are required. (See Section 3.2.8 for more information.)

2.2.7 Credential Evaluation Working Group (CEWG)

The CEWG is a group within the PMO that assembles periodically to address issues related to CS evaluation. Members of the CEWG are appointed by the PM. Responsibilities include:

1. CAF Suite changes. Any recommended changes to the CAF Suite of documents are the responsibility of the CEWG.

2. Application for Assessment. The CEWG makes the determination on whether to accept Applications for Assessments (see Section 3.1).

3. Determine Relative Assessment Priorities. The CEWG determines relative priorities for CS Assessment, which are factored into final Assessment schedule decisions made by the PM.

4. Assessor Qualifications. The CEWG will recommend to the PM criteria for Assessor designation that will include their required qualifications.

5. Ensure Assessment Consistency. The CEWG reviews the criteria adopted in the CAPs to ensure that Assessments are conducted consistently, even when subjective judgment is required by Assessors (see Section 3.2.4.3).

2.2.8 Federation User Group

The Federation User Group comprises representatives from each agency and CSP participating in the Initiative[1]. This user group has a vested interest in the CAF suite of documents because it pertains to assessment and approval of verifier services that the relying parties depend upon.

[1] Approved commercial-off-the-shelf product vendors may also be included.

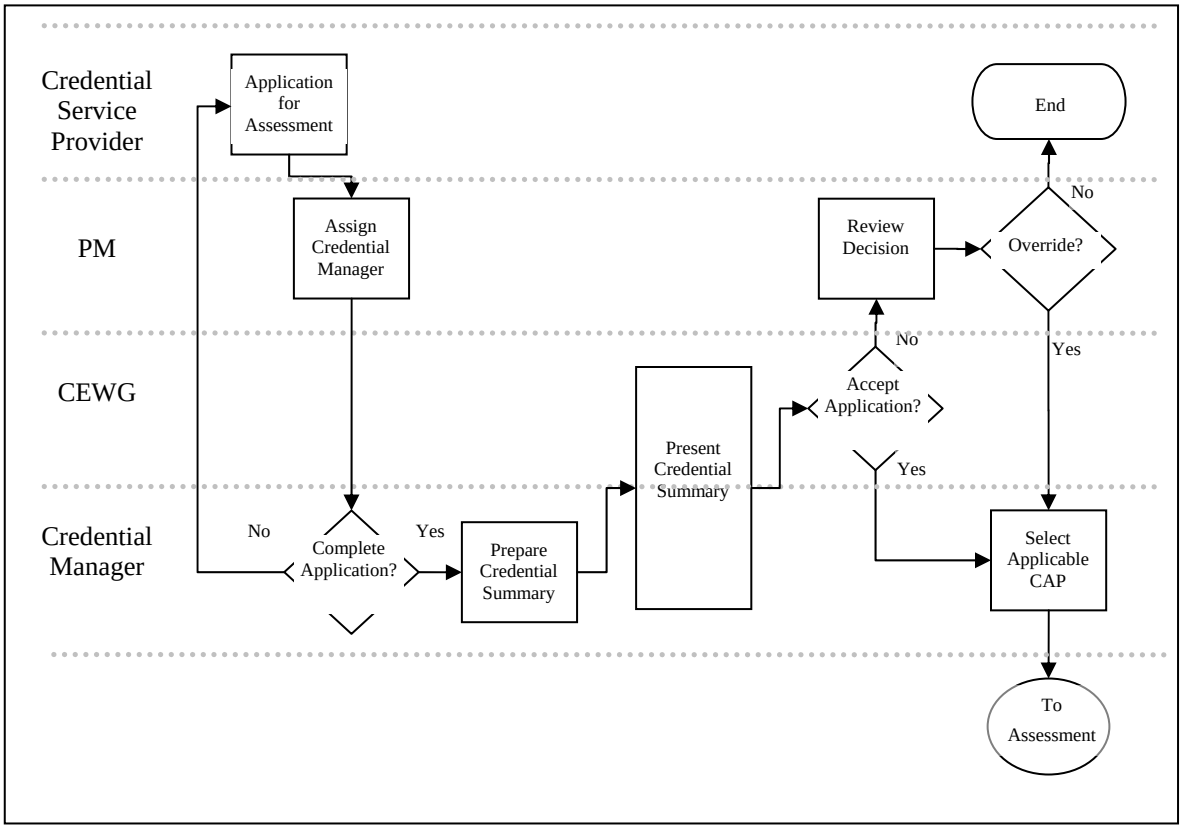
3 PROCESSES

This section describes the processes involved in making a CS available through the Initiative, which are the Application for Assessment, and the Assessment. CSPs must first apply to be assessed by submitting an Application for Assessment. If the application is accepted, the Assessment Team will be assigned to conduct the assessment.

3.1 Application for Assessment

The CSP application process is depicted in Figure 1. The goal of the application process is to help the PMO understand the CS, determine the business case and usefulness of the offer, and, with the recommendation of the CEWG, make a determination whether to proceed with a formal assessment.

Figure 1 CSP Application Process



3.1.1 Prepare Application for Assessment

The Credential Assessment process begins when the CSP submits an Application for Assessment to the PM. The E-Authentication website at http://www.cio.gov/eauthentication/ has templates and the latest guidance for application preparation, as well as the minimum requirements for consideration. A Planned CS is not eligible to apply; only services that are fully operational will be considered. Technical interoperability with the ASC is also required. Applicants should review the ASC Interface Specifications before applying. Applicants are encouraged to contact the PMO for informal discussions before preparing their application.

The goal of the application is to show the value proposition to the Government for the CS being offered. It should include the following elements:

1. A summary of the CS to be offered;
2. Potential benefits to the Government;
3. Technological basis of the credential and/or token (e.g., password, PIN);
4. Target Assurance Level;
5. The number of credentials in use;
6. Any demographics or descriptive information that is available about the credential holders;
7. Estimated time that will be required to complete the Assessment Package if the application is accepted;
8. Any audits that have been performed on the CS in the last year, including the auditing organization, the date of the audit, and the scope of the audit;
9. Adequate information to determine the legal and financial status of the CSP; and
10. The cost basis or charging mechanism that will be used.

3.1.2 Assign Credential Manager

Upon receipt of the Application for Assessment, the PM will assign a unique case number and Credential Manager to the application. Generally, the Credential Manager will be assigned based on their qualification and availability as well as the credential type and industry classification of the applicant. The Credential Manager will be the point of contact for the applicant and will coordinate all internal process activities.

The Credential Manager will notify the CSP that the Application for Assessment has been received. The Credential Manager will review the application for completeness and request an initial discussion with the CSP to develop the Credential Summary.

3.1.3 Prepare Credential Summary

Based on the Application for Assessment, the initial discussion and other information that may be obtained, the Credential Manager will develop the Credential Summary presentation. The goal of the Credential summary presentation is to provide the CEWG with enough information to make a decision without requiring everyone to study the Application for Assessment. This short presentation will capture the essence of the applicant's offering and the business case for inclusion in the Initiative. At a minimum, the presentation will include:

- Brief description of the CSP and the CS;
- Potential uses of credentials by Government agencies; and
- Known risks or liability issues.

The Credential Manager will schedule the presentation with the CEWG.

3.1.4 Present Credential Summary

The Credential Manager will present the Credential Summary to the CEWG and answer any questions. The CEWG will determine whether it is in the best interests of the Government to proceed with an Assessment. If an Assessment is warranted, the CEWG will also determine the relative priority of the CS, which will be factored into the PM's Assessment scheduling decisions. Priority decisions will be based on the overall value to the Government.

3.1.5 CEWG Decision Review

If the CEWG determines an Assessment is not warranted, the case will be reviewed by the PM. If the PM believes it is in the best interest of the Government, the PM can override the CEWG decision and call for an Assessment.

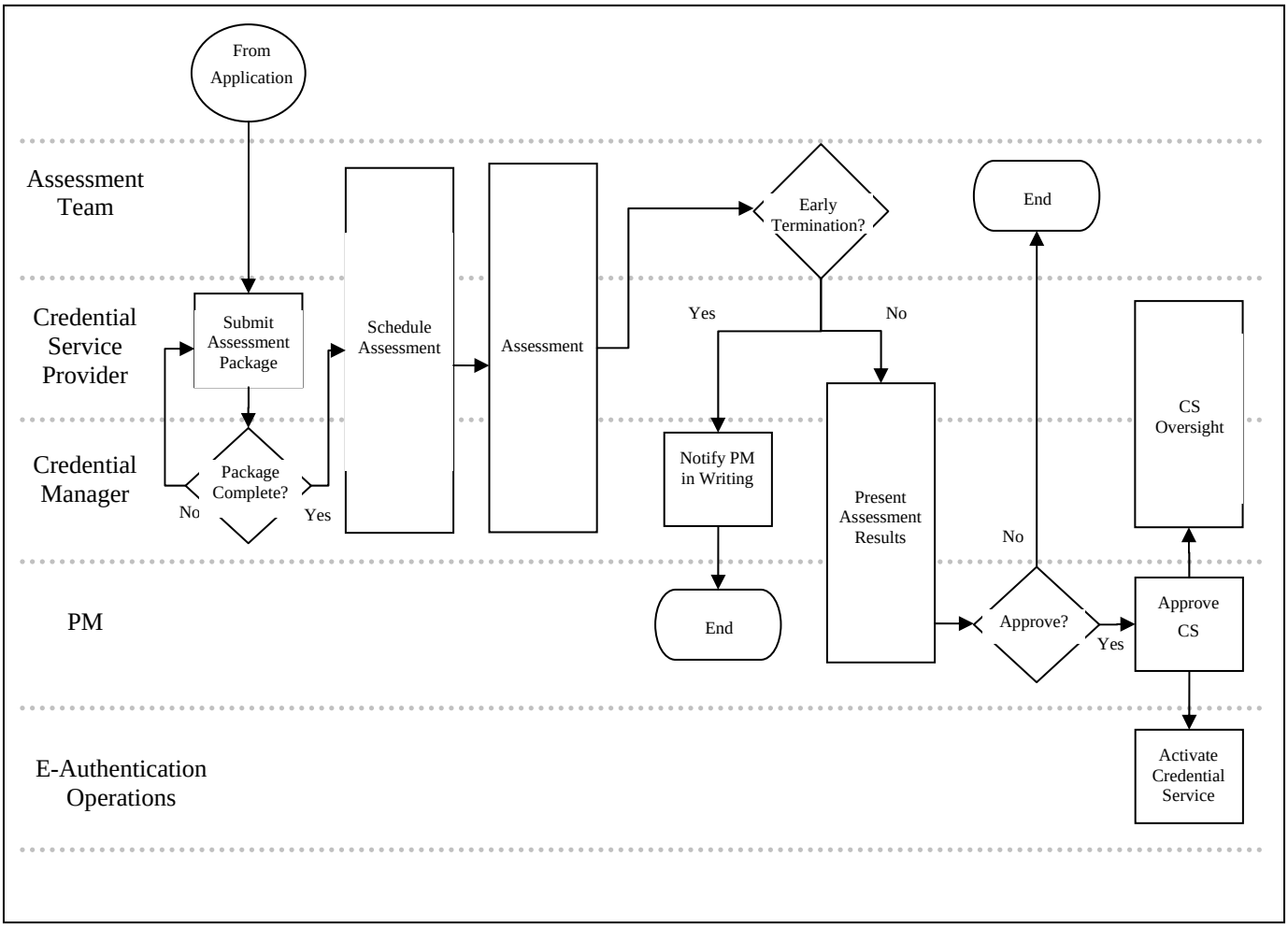
3.1.6 Select Appropriate Credential Assessment Profile

CAPs are used based on the credential type of the Candidate CSP. The Credential Manager will determine which CAP is applicable and notify the CSP. See Section 4 for more information on CAPs.

3.2 Assessment

The Assessment process is depicted in Figure 2. The goal of the Assessment process is to evaluate the CS against the applicable CAP to determine whether the credentials will be part of the Initiative, and if so, at what Assurance Level.

Figure 2 CSP Assessment Process



3.2.1 Submit Assessment Package

The Candidate CSP must complete and submit an Assessment Package to the Credential Manager. The Assessment Package contains the Evidence of Compliance for each criterion in the applicable CAP. Evidence could be in the form of an audit report or certificates from other external/independent assessments conducted by other parties within one year prior to package submission. It may be necessary to work with the Assessment

Team to develop a mutually acceptable list of evidence sufficient for the Assessment Team to determine the CS's compliance with the specified criteria.

The CSP is not required to submit all of their policies and procedures. The CSP need only submit sufficient information to evidence compliance with relevant criteria. In other words, sufficient information is required to enable the Assessment Team to make an informed decision.

Evidence of policies may not be considered sufficient. Evidence is required that actual practices are in line with policies. This may require site visits. Greater Assurance Levels claimed by CSPs may also elevate the need to corroborate actual practice and records with service claims and definitions.

A CSP may offer relevant evidence of a previous Assessment of some kind for all or part of its service. If this happens, Assessors shall form a judgment of the status and determine if the Initiative recognizes the competence of the previous Assessor.

Evidence may be provided by the Agency in cases where only a single Agency Application (AA) is using the CS. That is, CS and AA controls may be considered together so long as only one AA is using a CS. In the event that a CS is approved under this stipulation, that approval shall be rendered invalid should the CS be put into use by any additional AA(s).

3.2.2 Review Assessment Package

The Credential Manager will review the Assessment Package for completeness and responsiveness. They will then notify the CSP of their determination of whether or not to schedule an assessment.

3.2.3 Schedule Assessment

Working in coordination with Candidate CSP and the Assessment Team, the Credential Manager will schedule the Assessment. Target start and completion dates will be established along with a list of resources and information that will be required from the Candidate CSP.

3.2.4 Conduct Assessment

The Assessment Team will assess the practices of the Candidate CSP using the criteria established in the applicable CAP. 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.

A fundamental premise of the CAF is that CSPs (in particular, Assurance Level 2 and above) have likely undergone similar assessments (e.g., SAS 70, ISO 17799, WebTrust for CAs) or have processes that adhere to verifiable standards or best practices (e.g., ISO 9000 series). If a CSP has had previous independent assessments conducted of relevant aspects

of its service, Assessors must consider the relevance of the results of these assessments as evidence. For example, a CSP could satisfy the evidence requirements of an internal control by providing an appropriate ISO 9001 Certificate. However, if such an assessment has not been completed for a specific aspect of a CSP's service for which evidence is required, then the Assessment Team may have to conduct a more detailed examination such as reviewing a router configuration or a system event log. It is generally accepted that CSPs with Assurance Level 1 CSs may need not have undergone other assessments or audits.

The Credential Manager is not involved in the evaluation of evidence for criteria. The Credential Manager serves in a coordination role. Only Assessors from the assigned Assessment Team will determine compliance with criteria.

The Assessment Team and Credential Manager will prepare a written report containing the results of the Assessment. In addition to the findings from the Assessment, the team must provide a recommendation to the PM as to which Assurance Level the CS qualifies. The report will also be shared with the CSP, who will have time to comment on the report before it is provided to the PM.

Every CS is required to demonstrate interoperability with the ASC. The Assessment includes interoperability validation according to the latest ASC Interface Specifications (http://www.cio.gov/eauthentication/TechSuite.htm).

See the CAP Portfolio for more information.

3.2.4.1 Planning

Assessments are to be adequately planned. The first stage of the Assessment is planning. The Assessment Team should give consideration to the scope of the Assessment, as the CSP's service(s) requires and the extent and completeness of the evidence the CSP proposes. Based on this initial understanding, the Assessment Team should prepare a work plan that defines tasks, duration and resources, as well as the work methodology. In planning for the Assessment, the Assessment Team should:

- Consider the requirements of the Assessment Report;
- Carefully review the Application and Assessment Package submitted by the CSP;
- Identify and review results from other relevant assessments. Determine their validity and relevance to the Assessment, and the likely need for additional evidence to be determined;
- Prepare an Assessment Plan with milestones and schedule; and
- Conduct a Kick-off meeting with CSP and provide Assessment Plan.

3.2.4.2 Communication

Establish and maintain communication with the designated management of the CSP. From the onset, the Assessment Team should establish a line of communication with the CSP's Point of Contact. Once established, communication between the Assessment Team and CSP should, to the greatest extent, be in written form that includes the use of e-mail.

3.2.4.3 Subjective Judgment

Assessors are required to exercise a degree of subjective judgment when applying criteria to various CSPs. Despite the structure of the CAF and its associated CAPs, Assessors will have to rely on their experience and domain knowledge when determining a CSP's compliance to specific criteria. In addition, the rationale used by Assessors must be documented in the assessment results for review by the PM, and may be made available to the CSP. Documentation is necessary because issues of the intention of a criterion, or in what the Assessor considers persuasive evidence of compliance, may arise during assessments.

3.2.4.4 Close-out Meeting

The Assessment Team should conduct a close-out meeting with the CSP. The close-out meeting with the CSP signifies the end of the actual Assessment. During this meeting the Assessment Team should discuss the results of the Assessment to ensure that there has been no misinterpretation of evidence and to ensure that any required remedial actions have been adequately fulfilled by the CSP.

3.2.4.5 Assessment Report

The Assessment Team must prepare a written Assessment Report to document the approach, findings, and its recommendation regarding approval of the CS. Assessment Reports should be delivered to the assigned Credential Manager. The name of the CSP, the identity of the specific CS assessed, information gathered, analysis, results and recommendations shall not be disclosed outside the PMO for any reason. The Assessment Report must include:

- Assessment Objective. The Assessment Team should identify the CSP and state the identity of the CS being offered;
- Scope and Methodology. Based on the Assessment Objective, the Assessment Team should identify the CAP applicable to the CS, the sources of evidence and period of the Assessment. The Assessment Team should define the type of credential that is being offered, the claimed Assurance Level and explain the current use of the credential (e.g., online banking, Internet Service Provider);

- Findings. The Assessment Team should report the CSP's compliance with the criteria contained in the assigned CAP. For each criterion, the Assessment Team should identify the evidence provided, rationale for acceptance or rejection, and any deficiencies identified; and
- Approval Recommendation. Based on the scope and results of the Assessment, the Assessment Team must provide the PM with a recommendation for approval or rejection of the application, including their determination as to what Level of Assurance any approval should be granted.

If for any reason an Assessment is terminated, the Assessment Team should immediately provide written notification to the CSP and the Credential Manager. The Assessment Team must document the state of progress of the Assessment at the time of termination and explain why the Assessment was terminated.

3.2.5 Present Assessment Results

The Credential Manager will present the final Assessment results, along with a recommendation, to the PM.

3.2.6 Evaluate Results

Based on the Assessment Report presented by the Credential Manager, the PM will make the final ruling on the CS. The PM will review the results to ensure the Assessment has been properly conducted and then, barring any exceptions, grant Approval for the CS.

3.2.7 Approve CS

The PM will provide approval to operate as a trusted CS through executing a service agreement with the CSP for the approved CS at the determined Assurance Levels. The template CSP service agreement is available at http://www.cio.gov/eauthentication/.

3.2.8 Credential Maintenance

The CSP must notify the Credential Manager of any material changes (i.e., changes the status of evidence from compliant to non-compliant) on the CS that may affect the Assurance Level of the CS 60 days before the changes are performed. The PM will determine whether the changes are sufficient to require re-assessment. Any change-driven re-assessment would only cover those elements that have changed.

The PM may require a re-assessments if updates to the applicable CAP may affect the Assurance Level of the CS. The re-assessment would only cover the criteria that were changed in the CAP update.

Annual renewal agreements are required for a CS to remain approved. The CSP states continued compliance with the criteria of their assessment in this agreement, and provides annual audit results. An independent third party must audit a CS assessed at Assurance

Level 2 or higher every two years. Other audits may be internal. The PM may require a partial re-assessment if the scope of the audits do not include all applicable criteria.

Additional maintenance activities may be stipulated in the service agreement between the PMO and the CSP.

In general, all requirements of the on-going relationship will be specified in the participation agreement, including maintenance requirements.

3.2.9 Activate Credential Service

Once the CS is approved to operate, the E-Authentication Operations team will place the CS on the E-Authentication Trust List, which is available at http://www.cio.gov/eauthentication/ TCSPlist.htm.

4 CREDENTIAL ASSESSMENT PROFILES

4.1 Description

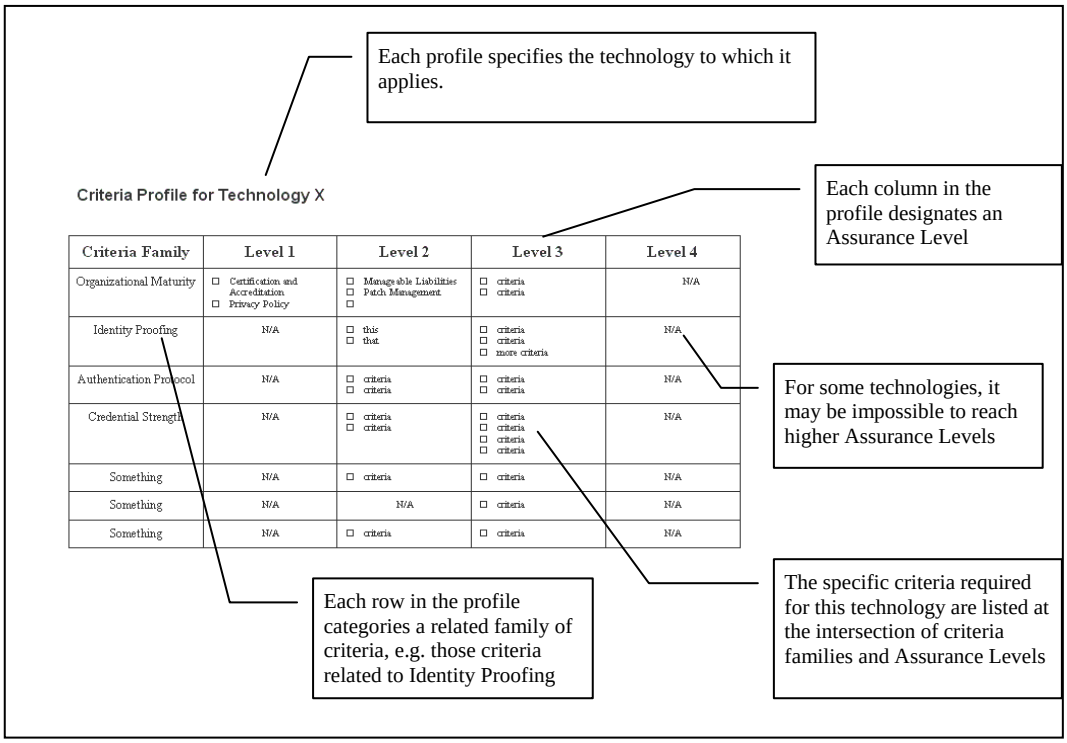
The specific requirements for a CS to be assessed at a particular Assurance Level are expressed in CAPs. The Initiative has multiple CAPs and is expected to add additional CAPs over time. The Password CAP establishes requirements that are standard across any Password CS (i.e., Password and PIN). The Certificate CAP covers certificate-based CSs (i.e., public key certificates). Additional CAPs may be defined over time for different types of CSPs, such as banks or Government agencies.

Each individual criterion is named and defined in each CAP. The criteria are divided into families of related requirements, such as identity proofing or authentication protocol. Using the criteria in the applicable CAP, the Assessment Team evaluates and assesses evidence relating to a CSP's general business practices, security and internal controls. Generally, each CAP criterion addresses one of the following areas:

- Presence and maturity of written business practices;
- Presence of a Business Continuity Plan and the organization's readiness to respond and recover from an emergency;
- Presence of and adherence to information security policies and practices;
- Network and system security;
- Ability to interoperate with the E-Authentication Service;
- Subscriber Agreements;
- Strength and resilience of credentials and tokens; and
- Rigorousness of registration and record retention.

The CAP also defines which criteria are required for each Assurance Level. Figure 3 shows an example criteria CAP.

Figure 3 Example Criteria CAP



Criteria Family	Level 1	Level 2	Level 3	Level 4
Organizational Maturity	☐ Certification and Accreditation ☐ Privacy Policy	☐ Manageable Liabilities ☐ Patch Management ☐	☐ criteria ☐ criteria	N/A
Identity Proofing	N/A	☐ this ☐ that	☐ criteria ☐ criteria ☐ more criteria	N/A
Authentication Protocol	N/A	☐ criteria ☐ criteria	☐ criteria ☐ criteria	N/A
Credential Strength	N/A	☐ criteria ☐ criteria	☐ criteria ☐ criteria ☐ criteria ☐ criteria	N/A
Something	N/A	☐ criteria	☐ criteria	N/A
Something	N/A	N/A	☐ criteria	N/A
Something	N/A	☐ criteria	☐ criteria	N/A

CSPs prepare their submission by providing Evidence of Compliance to satisfy each criterion in the applicable CAP. The Assessment Team then validates the evidence for each criterion for the target Assurance Level. All criteria for lower Assurance Levels must also be satisfied. The ultimate recommended Assurance Level for the CS is the Assurance Level for which all criteria have been validated, including lower Assurance Levels.

4.2 CAP Development

Technology changes rapidly and authentication technology is no exception. As new technologies become available and show promise for the Initiative, the CEWG will oversee the preparation of new CAPs that will in turn be submitted to the PMO for approval. In addition, new CAPs being drafted will be made available to various Government agencies and organizations, including CSPs, for comment. Those comments will be provided to the CEWG before the CAPs are approved. See Appendix A for an overview of the overall change and approval process flow.

4.3 CAP Maintenance

The Initiative will evolve over time. As the needs of the Initiative change or become clearer, it is likely that CAPs will evolve. The CEWG has responsibility for CAP maintenance. Revised CAPs being drafted will be made available to various Government agencies and organizations, including CSPs, for comment. Those comments will be provided to the CEWG before the CAPs are approved. The CAPs must be approved by the PMO before they become effective. See Appendix A for an overview of the overall change and approval process flow.

5 REFERENCES

[ANSI X9.79] "American National Standard for Financial Services - Part 1: PKI Practices and Policy Framework", ANS X9.79-1:2001,

[BS 7799-2] "Information Security Management - Part 2: Specification for information security management systems", 1999, published by the BSI, ISBN 0 580 28280 5.

[FIPS-140-2] "Security Requirements For Cryptographic Modules", Federal Information Processing Standard Publication 140-2, 1999.

[EA-7/03] "EA Guidelines for the Accreditation of bodies operating certification / registration of Information Security Management Services", 2000.

[ISO 9001-2000] "Quality management systems -- Requirements" 2000-12-08

[ISO/IEC G62] ISO/IEC Guide 62:1996 "General Requirements for Bodies Operating Assessment and Certification/ Registration of Quality Systems"

[ISO/IEC 17799] "Information technology - Code of practice for information security management", ISO/IEC 17799:2000, first edition, 2000-12-01.

[OCSP] "Internet X.509 Public Key Infrastructure Online Certificate Status Profile" (RFC 2560) Feb 2002.

[PKCS #5] "Password-Based Cryptography Standard", RSA Laboratories, v2.0, March 25, 1999

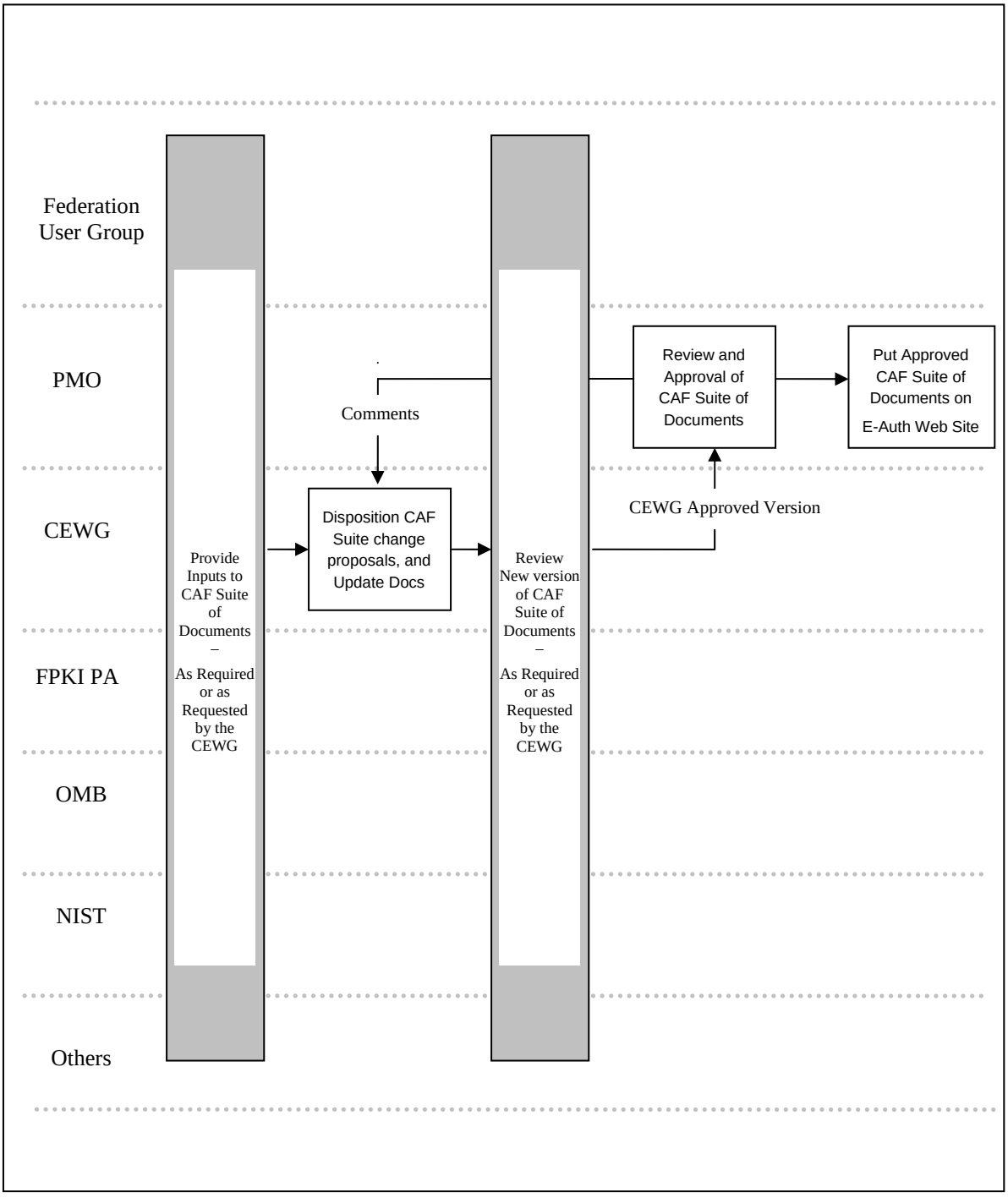
[QCP] "Policy requirements for certification authorities issuing qualified certificates", ETSI TS 101 456.

[X.509] "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU Recommendation X.509. (03/00)

[M-04-04] The OMB E-Authentication Guidance

[SP 800-63] NIST Special Publication 800-63 version 1.0.1

Appendix A CAF Suite Change and Approval Process



Appendix B Glossary

Term	Definition
Address of Record	The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.
Application for Assessment	A package submitted by CSPs who wish to make a CS available for use in the Initiative. See Section 3.1.1.
Approval	In context of E-Authentication Initiative participation - authority to operate.
Approved	FIPS approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation. Approved cryptographic algorithms must be implemented in a crypto module validated under FIPS 140-2. For more information on validation and a list of validated FIPS 140-2 validated crypto modules see http://csrc.nist.gov/cryptval/.
Assertion	A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.
Assessment Package	A package submitted by CSPs who have been accepted for assessment. The package contains evidence of compliance with all applicable criteria. See Section 3.2.1.

Term	Definition
Assurance Level	Level of trust, as defined by the OMB Guidance for E-Authentication. This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four levels of assurance are: Level 1: Little or no confidence in the asserted identity's validity. Level 2: Some confidence in the asserted identity's validity. Level 3: High confidence in the asserted identity's validity. Level 4: Very high confidence in the asserted identity's validity.
Asymmetric Keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Authentication	The process of establishing confidence in user identities.
Authentication Protocol	A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
Authentication Service Component (ASC)	A federated architecture that leverages credentials from multiple domains through certifications, guidelines, standards adoption and policies. The ASC accommodates assertion-based authentication (i.e., authentication of PINs and Passwords) and certificate-based authentication (i.e., public key certificates) within the same environment. Over time, the architecture will leverage multiple emerging schemes such as the SAML and Liberty Alliance, and will not be built around a single scheme or commercial product. In this light, the ASC is more precisely defined as an architectural framework.
CAP Portfolio	The portfolio of Credential Assessment Profiles, i.e. all approved profiles.
Claimant	A party whose identity is to be verified using an authentication protocol.

Term	Definition
Credential	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Note that this document uses "credential" broadly, referring to both electronic credentials and tokens.
Credential Assessment Profile (CAP)	A list of related criteria used to *assess* the Assurance Level of a Credential Service. The E-Authentication Initiative has several CAPs.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential then each one is considered a separate CS.
Credential Service Provider (CSP)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.
Cryptography	The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof. [ANSI X9.31] Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption. [NIST SP 800-2]
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number.
Cryptographic Strength	A measure of the expected number of operations required to defeat a cryptographic mechanism. For the purposes of this document, this term is defined to mean that breaking or reversing an operation is at least as difficult computationally as finding the key of an 80-bit block cipher by key exhaustion that is it requires at least on the order of 279 operations.
Cryptographic Token	A token where the secret is a cryptographic key.
Digital Signature	An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.

Term	Definition
Electronic Credentials	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token.
Entropy	A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. Guessing entropy is a measure of the difficulty that an attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution.
Federal Bridge Certification Authority (FBCA)	Allows PKIs to trust digital certificates issued by other entities that have been policy mapped and cross-certified with the FBCA. See http://www.cio.gov/fpkipa/.
Federal Public Key Infrastructure (FPKI)	Employs a FBCA to harmonize policies and procedures for CAs. See http://www.cio.gov/fpkipa/.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKI Policy Authority sets policy governing operation of the FBCA and approves applicants for cross certification with the FBCA. The FBCA allows discrete Public Key Infrastructures (PKI) to trust digital certificates issued by other entities that have been policy mapped and cross-certified with the FBCA. The FPKI Policy Authority is composed of organizations that wish to interoperate and exchange digital certificates that have been signed by their Certification Authority with the FBCA. Determinations by the FPKI Policy Authority apply to the issuance of cross-certificates to approved participants but does not prescribe how those entities are to rely on digital certificates for transactions; all entities are free to accept or reject any digital certificate issued by any other entity at their sole discretion, using available FPKI Policy Authority determinations to assist in making informed decisions.

Term	Definition
Federal Identity and Credentialing Committee (FICC)	The FICC will make policy recommendations and develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture, to include associated services (identity proofing, credential management, etc.), for the Federal Government. Objectives are: • Simplify and Unify Identity Authentication for Federal Employees • Create requirements for Physical Credentials, electronic credentials, and issuance. • Develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture
Governing Authority	Established by the government to issue certificates that allow Agency Applications to retrieve SAML assertions from Credential Services over a client and server authenticated SSL channel, effectively controlling which entities can participate.
Identity	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
Identity Proofing	The process by which a CSP and an RA validate sufficient information to uniquely identify a person.
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. See also PIN.
Personal Identification Number (PIN)	A password consisting only of decimal digits.
Program Management Office (PMO)	Established by the government to issue certificates that allow Agency Applications to retrieve SAML assertions from Credential Services over a client and server authenticated SSL channel, effectively controlling which entities can participate.
Possession and control of a token	The ability to activate and use the token in an authentication protocol.
Proof of Possession (PoP) protocol	A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password).
Protocol Run	An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant.

Term	Definition
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See also [RFC 3280].
Registration	The process through which a party applies to become a subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP.
Registration Authority	A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Relying Party	An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.
Shared Secret	A secret used in authentication that is known to the claimant and the verifier. There are two durations for a shared secret: • Session (temporary) secret – duration of the secret is limited to the duration of the user session. That is, the secret is created, used, and expired during a single user authentication session. • Long-term secret – duration of the secret persists ongoing, and is used from one user authentication session to another user authentication session.
Subject	The person whose identity is bound in a particular credential.
Subscriber	A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol.
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.
Trust List	The list of authorized CSs and their associated assurance levels comprise the Trust List.
Verified Name	A subscriber name that has been verified by identity proofing.
Verifier	An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status.

Appendix C Acronyms

Term	Definition
AA	Agency Application
ANSI	American National Standards Institute
ASC	Authentication Service Component
CA	Certification Authority
CAF	Credential Assessment Framework
CAP	Credential Assessment Profile
CEWG	Credential Evaluation Working Group
CS	Credential Service
CSP	Credential Service Provider
EA	European Co-operation For Accreditation
ESC	Executive Steering Committee
FBCA	Federal Bridge Certification Authority
FICC	Public Key Infrastructure
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
FPKI PA	Federal Public Key Infrastructure Policy Authority
FTS	Federal Technology Service
GSA	General Services Administration
ISO	International Organization For Standardization
NIST	National Institute Of Standards And Technology
OCSP	Online Certificate Status Protocol
OMB	Office Of Management And Budget
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
PoP	Proof of Possession
RA	Registration Authority
RFC	Request For Comment
SAML	Security Assertion Markup Language
SAS	Statement On Auditing Standards

Term	Definition
SSL	Secure Socket Layer

Appendix D Detailed Document History

Status	Release	Date	Comment	Audience
Draft	1.0.0	7/10/03	First release	Limited
Interim	1.3.0	12/19/03	Released for customer review with the proposal that it be accepted for publication as 2.0.0: ▪ §1.3 Remove references to this document; ▪ §1.2, 1.3 - Drafting amendments to refer to NIST SP 800-63 Nov03 AND minor proofing amendments which have changed neither the semantics nor the intentions of the document. ▪ NB - this document supersedes 1.1.0, which was overtaken by release of the Nov. 2003 draft of NIST SP 800-63 and withdrawn before release.	Customer
Interim	1.4.0	3/1/04	CP #74 - Change CAP references to cite Non-PKS and PKS CAPs, as a result of consolidating Common, PIN, Password CAPs into a single Non-PKI CAP)	Sill, Terango, Louden
Draft	1.5.0	1/14/05	Changes per CAF Suite change proposal matrix approved by the CEWG. Changes include: • Add hyperlink formatting to web addresses • Added Acronyms as Appendix C. • Added additional PM role of assigning unique case number to each application, per section 3.1.2. (§2.2.3) • Added new document link (§3.2.9). • Change “initiative” to “Initiative” throughout. • Change alternate references to “CAP”, such as “profile” to “CAP” - to have consistent citation throughout document. • Change section references (‘see section 3.2’ to ‘see section 3.2.1’) to be more specific as the relevant section (§2.2.6, Appendix B). • Change some document links, to make them more precise as to the location (§1.2, §3.2.4) • Convert to acronyms throughout. • Grammar and syntax changes where appropriate. • Make references to roles consistent throughout, per names defined in §2.2 • Moved Executive Summary from the cover page to it own page because it is too long for the cover page. • Moved terminology listing from §1.1 to Appendix B because the listing is so long. • CP # 2 - Add “version 1.0.1” to all references of NIST SP 800-63 • CP # 57 - Delete “Interim”; Do not replace with “FOC” • CP #51 - Revise and extend special terms	FSTC Working Group for feedback, via Georgia Marsh

Status	Release	Date	Comment	Audience
			section (§1.1), to align with NIST SP 800-63. Add definitions that will be useful in this document and other Suite documents to provide additional background, as necessary. • CP #58 - Change "PKI based" to "certificate based" • CP #58 - Change CAP references to "Password CAP" and Certificate CAP" (as a result of consolidating the PIN, Password and Common CAPs into as single CAP called "Password CAP", and changing "PKI CAP" to "Certificate CAP"). • CP #59 – Change "Gateway Operations" to E-Authentication Operations" in "Assessment" section (§3.2), Figure 2. • CP #62 – Added additional PM role for clarity as to who determines the assessment schedule. (§2.2.3). Also add clarification in main discussion (§3.1.4) • CP #66 – Add Entropy Spreadsheet to the list of items in the CAF Suite cited in the Related Documents section (§1.2) • CP #67 - Move text in "CAP Maintenance" (§4.3) pertaining to new CAP development to "CAP Development" (§4.2). • CP #71 – Add clarification to "Introduction" (§1) that processes specified herein are mandatory except for those items that explicitly grant latitude or judgment. • CP #72 - Reword "Assessment Team" section (§2.2.5) for a more complete description. • CP #75 - Change "E-Authentication Service" to "Authentication Service Component" • CP #75 – In "Prepare Application for Assessment section (§3.1.1), Change "E-Authentication Architecture" to "Authentication Service Component" • CP #86 - Added scope of E-Authentication as remote electronic authentication of human users…. (§1) • CP #94 – change "against criteria established in the CAF" to "against criteria established in the CAF Suite". (§1) • CP #96 – Make "Profiles" and CAPs" singular, throughout the document, as appropriate. • CP #97 - Changed "Designated Assessor" to "Assessor" throughout the document, to be consistent throughout (most other references use "Assessor"). • CP # 99a - Add new section 2.2.5.1, "Assessor	

Status	Release	Date	Comment	Audience
			Qualifications". • CP #100 - Added new CEWG role to clarify that CEWG determines relative assessment priorities, but that the relative priorities are inputs to the PM who makes final Assessment schedule decisions. (§2.2.7) • CP #101 – rework "Prepare Credential Summary" section by moving objectives statement to the beginning, and deleting ", make the presentation, and answer any questions" because it is relevant in the next section, and is already stated in the next section. (§3.1.3) • CP #103 – change "PMO" to "Credential Manager". (§3.2.8) • CP #104 - Added additional Credential Manager role, per section 3.2.4.5, which discusses Assessment termination. (§2.2.4) • CP #104 – In the discussion about Assessment termination, change "PMO" to "Credential Manager", as the Credential Manager oversees the Assessment process and interacts with the CSP. (§3.2.4.5) • CP # 104 – Change Figure 2 to include sub flow if the Assessment is terminated early. (§3.2) • CP # 105 – in "CAP Development" section, change "ESC" to "CEWG" regarding flow of comments from CSPs, to be consistent with new content approval flow diagram. (§4.3) • CP # 105 – Add clarification to CAP Development that approval process is PMO first, then final by ESC Relying Party User Group. (§4.2, §4.3) • CP #105 – Added Appendix A to highlight overall CAF Suite change and approval process flow. (§Appendix A) • CP #108 – changed "PMO" to "PM" in the sentence "A Credential Manager is assigned by the PM to manage this process." (§1.3) • CP #109 – Change "PMO" to "PM". (§3.1.1, §3.1.2, §3.2.8) • CP #110 – Added additional role that PM can override CEWG's decision to reject an application, per Figure 1. (§2.2.3) • CP #111 – Added additional role for Credential Manager that CM determines applicable CAP and notifies CSP, per section 3.1.6 (§2.2.4) • CP #112 – change Figure 1, bottom, right bubble, to indicate "To Assessment" • CP #114 - Added Credential Manager step at	

Status	Release	Date	Comment	Audience

			the beginning to check whether application is complete, and arrow back to CSP if not complete. (§3.1)
			• CP #117 - Add clarification that audit report or certificates must be within one year prior to package submission (§3.2.1)
			• CP #118 - Extended Figure 2 "Schedule Assessment" box to include CSP and Assessment team, as discussed in section 3.2.3. (§3.2)
			• CP #119 – Change "conformity" to "compliance" (§3.2.4, §3.2.4.3)
			• CP #124 – change variants of "authorize" to corresponding variant of "approve" throughout the document.
			• CP #125 – Add additional PM role regarding determination of need for re-assessment. (§2.2.3)
			• CP #126 - Change MOU and MOA to "participation agreement" (§2.2.2, §3.2.8)
			• CP #128 – Update "CAP Development" section to clarify scope of feedback returned to the CEWG, per the newly added CAF Suite change/approval process flow. (§4.2)
			• CP #128 – Update "CAP Maintenance" section to clarify scope of feedback returned to the CEWG, per the newly added CAF Suite change/approval process flow. (§4.3)
			• CP #70 – fully integrated CAG throughout this document, as appropriate:
			  • Delete all references to CAG, as it is no longer a separate document (§1.2, §2.2.3, §2.2.5, §2.2.6, §3.2.4)
			  • Add bullet list of CAP criteria §4.1
			  • "Submit Assessment Package" (§3.2.1) reworked by integrating CAG section 2.2.
			  • "Conduct Assessment" (§3.2.4), added text from CAG discussing external, independent audits.
			  • "CEWG" (§2.2.7), added additional role of recommending Assessor qualifications.
			  • "Program Manager" (§2.2.3), added additional responsibility of maintaining list of active and approved Designated Assessors.
			  • "Assessment Team" (§2.2.5), added discussion of Assessor independence, NDA, and conflicts of interest.
			  • "Assessor Qualifications" (§2.2.5.1), added first three bullets for minimum Assess Team requirements.	

Status	Release	Date	Comment	Audience
			• Added new section "Planning" (§3.2.4.1) • Added new section "Communication" (§3.2.4.2) • Added new section "Subjective Judgment" (§3.2.4.3) • Added new section "Close-out Meeting" (§3.2.4.4) • Added new section "Assessment Report" (§3.2.4.5) • Add comments to "Executive Summary" • Revise wording in "General Approach" (§1.3) regarding PM final review of assessment, and Authorization to Operate. • Revise wording in "Introduction" (§1) regarding assessments in a consistent, complete, and professional manner. • Added to "Program Manager" (§2.2.3), qualification that designation of assessors is "based on qualification criteria." • Add text to "Introduction" (§1) stating that processes discussed are based on best practices GAO principles and standards. • Added new section 5, "References" • Added additional CEWG role, "Ensure Assessment Consistency" (§2.2.7)	
For Approval	1.6.0	1/17/05	• Change "E-Authentication Initiative" to "Initiative" for consistency.	CEWG
For Approval	1.7.0	1/4/05	• Figure 2, extend "Present Assessment Results" upwards to include CSP. (§3.2) • Indicate that the PMO provides final approval for CAF Suite changes. (§1.3, §2.1, §2.2.2, §3.2, §3.3) • Indicate that ESC provides funding to the Initiative, and receives status reports from the PMO (§2.2.1) • Change "ESC Relying Party User Group" to "Federation User Group", which includes agencies and CSPs (and possibly approved COTS vendors). Move section 2.2.1.1 to section 2.2.8, as the user group is not directly related to the ESC. • Appendix A, change "ESC Relying Party User Group" to "Federation User Group. • Appendix A, change to indicate that PMO has final approval of CAF Suite changes.	PMO
PMO Approved	2.0.0	3/16/05	Approved by the PMO	Public