



# **E-Authentication**

## **Interim Credential Assessment Framework**

### **(CAF)**

12/19/2003  
release 1.3.0

## **Executive Summary**

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

The E-Authentication Initiative maintains a Trust List, which contains the Credential Services (CSs) that can be used by the initiative. CSPs go through an application process before they are assessed. The assessment process is governed by 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.

## **Release Notes**

*Interim Release*

## 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: <ul style="list-style-type: none"><li>▪ §1.3 Revision to remove references to this specific document;</li><li>▪ §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.</li><li>▪ NB - this document supersedes 1.1.0, which was overtaken by release of the Nov. 2003 draft of NIST SP 800-63 and withdrawn before release.</li></ul>	Customer

## Editors

Chris Louden  
Kevin Hawkins  
Richard G. Wilsher  
Dave Silver

Judy Spencer  
David Temoshok  
Steve Timchak  
Von Harrison

Bill Burr  
John Cornell  
Stephen Sill

# Table of Contents

- 1 INTRODUCTION..... 1**
- 1.1 SPECIAL TERMS ..... 2
- 1.2 RELATED DOCUMENTS..... 2
- 1.3 GENERAL APPROACH..... 3
- 2 INTERIM GOVERNANCE ..... 5**
- 2.1 GOVERNING ORGANIZATIONAL STRUCTURE..... 5
- 2.2 ROLES AND RESPONSIBILITIES..... 5
  - 2.2.1 *Executive Steering Committee (ESC)* ..... 5
  - 2.2.2 *Program Management Office (PMO)*..... 5
  - 2.2.3 *Program Manager (PM)* ..... 5
  - 2.2.4 *Credential Manager* ..... 6
  - 2.2.5 *Assessment Team*..... 6
  - 2.2.6 *CSP*..... 6
  - 2.2.7 *Credential Evaluation Working Group (CEWG)*..... 7
- 3 PROCESSES ..... 8**
- 3.1 APPLICATION FOR ASSESSMENT ..... 8
  - 3.1.1 *Prepare Application for Assessment*..... 9
  - 3.1.2 *Assign Credential Manager*..... 9
  - 3.1.3 *Prepare Credential Summary*..... 9
  - 3.1.4 *Present Credential Summary*..... 10
  - 3.1.5 *CEWG Decision Review*..... 10
  - 3.1.6 *Select Appropriate Credential Assessment Profiles* ..... 10
- 3.2 ASSESSMENT ..... 11
  - 3.2.1 *Submit Assessment Package*..... 11
  - 3.2.2 *Review Assessment Package*..... 12
  - 3.2.3 *Schedule Assessment* ..... 12
  - 3.2.4 *Conduct Assessment* ..... 12
  - 3.2.5 *Present Assessment Results* ..... 13
  - 3.2.6 *Evaluate Results* ..... 13
  - 3.2.7 *Authorize CS*..... 13
  - 3.2.8 *Credential Maintenance* ..... 13
  - 3.2.9 *Activate Credential Service* ..... 13
- 4 CREDENTIAL ASSESSMENT PROFILES ..... 14**
- 4.1 DESCRIPTION ..... 14
- 4.2 PROFILE DEVELOPMENT..... 15
- 4.3 PROFILE MAINTENANCE..... 15

## Figures

- Figure 1 CSP Application Process ..... 8
- Figure 2 CSP Assessment Process ..... 11
- Figure 3 Example Criteria Profile ..... 14

## **1 INTRODUCTION**

This document describes the processes involved in making individual identity credentials available to the E-Authentication Initiative. The E-Authentication project, 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.

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) against criteria established in the CAF.

## 1.1 Special Terms

This document relies on terminology defined in NIST SP 800-63 ‘Recommendations for Electronic Authentication’ (Nov. 2003) and the OMB ‘Guidance for E-Authentication’. The following terms have special meaning in this context:

Term	Definition
Credential	Digital documents used in authentication and access control that bind an identity or an attribute to a claimant’s token or some other property such as his or her current network address. Note that this guidance distinguishes between credentials, and tokens (see below) while other documents may lump tokens with credentials.
Claimant	A party whose identity is to be verified using an authentication protocol.
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)	An organization that offers one or more Credential Services (CSs).
Assurance Level	Level of trust, as defined by the OMB Guidance for E-Authentication.
Trust List	The list of authorized CSs and their associated assurance levels comprise the Trust List.
Credential Assessment Profile (CAP)	A list of related criteria used to <i>assess</i> the Assurance Level of a Credential Service. The E-Authentication initiative has several CAPs.
CAP Portfolio	The portfolio of Credential Assessment Profiles, i.e. all approved profiles.
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.
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.
Token	Something that the claimant possesses or knows (typically a key or password) that can be used to remotely authenticate the claimant’s identity. Technically, the token includes a userid and password that ensures token uniqueness within a credential domain.
Authorization	Authority to Operate.

## 1.2 Related Documents

The Office of Management and Budget (OMB) E-Authentication Guidance and NIST SP 800-63 documents establish the E-Authentication Assurance Levels and their technical requirements. 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 Interim Credential Assessment Profiles (CAPs), which are described in Section 4.

The E-Authentication Interim Credential Assessment Guidance (CAG) provides guidance on Assessments.

The E-Authentication Service Interface Specifications describe the requirements for CSPs to interoperate with the E-Authentication Initiative. The most recent version of these documents can be found at <http://www.cio.gov/eauthentication/>.

The CAF, CAG, and CAPs (Common, Password, PIN and PKI) currently comprise the CAF Suite, which governs the E-Authentication Initiative. The CAF Suite listing is maintained on the E-Authentication website (<http://www.cio.gov/eauthentication/>).

### **1.3 General Approach**

The E-Authentication 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 Credential Services that have been evaluated for use by the Federal Government. Each of these Credential Services is assessed to a particular Assurance Level as defined by the OMB and NIST Guidance documents. The list of assessed CSs that have been authorized and their associated Assurance Levels comprise 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 Credential Service Provider (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 CAPs. The CSP must submit evidence that shows compliance for each of the criteria elements in the applicable profiles. The evidence is then validated by Assessment Teams, which are designated by the E-Authentication 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.

A Credential Manager is assigned by the Program Management Office (PMO) to manage this 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 Credential Assessment Profiles (CAPs) may be developed by the initiative. The Executive Steering Committee (ESC) must approve each profile before it becomes effective.

## **2 INTERIM GOVERNANCE**

### **2.1 Governing Organizational Structure**

The E-Authentication Initiative is governed by the ESC which is comprised of executives from each of the agencies involved in the initiative. GSA is the managing partner for the E-Authentication Initiative, and the PMO is run by GSA 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 PKI credentials. The E-Authentication initiative uses PKI certificates, but defers their governance to the FPKI PA. The E-Authentication Assurance Levels for PKI 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 PKI Credential Assessment Profile describes specific mapping for PKI CSs to E-Authentication Assurance Levels.

### **2.2 Roles and Responsibilities**

The following section provides the roles and responsibilities involved in governance of E-Authentication CSs.

#### **2.2.1 Executive Steering Committee (ESC)**

The ESC is an intergovernmental committee comprised of executives from each agency participating in the E-Authentication 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 must approve the policies and procedures governing the initiative before becoming effective.

#### **2.2.2 Program Management Office (PMO)**

The PMO is the organization within GSA that handles program management, administration, and operations for the initiative. All contracts, licensing, and memoranda of agreement (MOA) related to the initiative are executed and managed by the PMO.

#### **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. Credential Manager responsibilities are described below.
3. Designation of Assessors. The PM determines who is approved to perform assessments for the initiative. See the Credential Assessment Guidance (CAG) for more information.

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. Any given 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 Credential Evaluation Working Group (CEWG) and determine which CAPs are appropriate if the application is accepted.
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. CS Maintenance. Every CS on the Trust List has a Credential Manager assigned to ensure appropriate maintenance responsibilities are met.

#### **2.2.5 Assessment Team**

The Assessment Team is comprised of Assessors designated by the PM to evaluate a CSP against the applicable CAPs. Additional information on Assessments is available in Section 3.2 and the Interim Credential Assessment Guidance. 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 team believes the CS should be included on the Trust List, and if so, at which Assurance Level.

#### **2.2.6 CSP**

Credential Service Provider, 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 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 their Assessment Package, which includes evidence of compliance with the appropriate CAPs. (See Section 3.2)
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 the Interim Credential Assessment Guidance and 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. Any recommended changes to the CAP portfolio or the Guidance for Assessors are vetted through this group. The CEWG also makes the determination on whether to accept Applications for Assessments. (See Section 3.1).

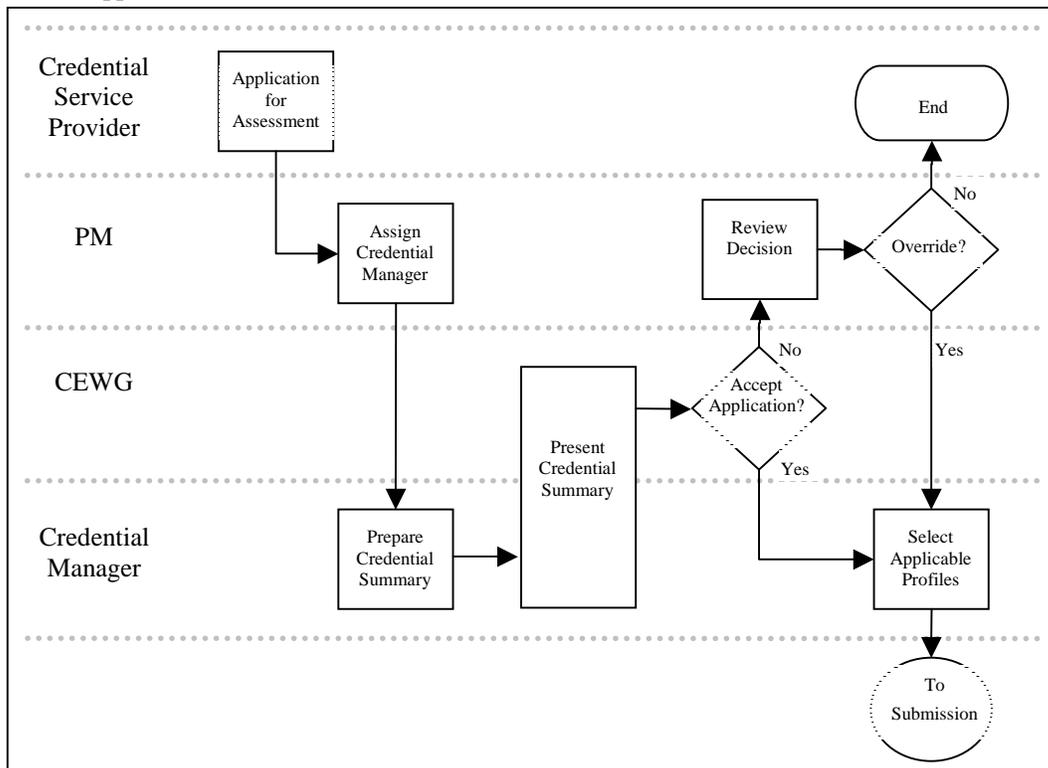
### 3 PROCESSES

This section describes the processes involved in making a CS available through the E-Authentication initiative. There are two parts in the process, application for assessment, and assessment. CSPs must first apply to be assessed by submitting an Application for Assessment. If the application is accepted then the CS is allowed to go through the assessment process.

#### 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 make a determination whether to proceed with a formal assessment.

Figure 1 CSP Application Process



### **3.1.1 Prepare Application for Assessment**

The process begins when the CSP submits an Application for Assessment to the PMO. 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 E-Authentication Service is also required. Applicants should review the 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 (password, PIN, etc);
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; and
9. Adequate information to determine the legal and financial status of the CSP.

### **3.1.2 Assign Credential Manager**

Upon receipt of the Application for Assessment, the PMO will assign a unique case number and Credential Manager to the application. Generally, the Credential Manager will be assigned based on their 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 of the PMO's receipt of the application. 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. This short presentation captures the essence of the applicant's offering and the business case for inclusion in the E-Authentication 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, make the presentation, and answer any questions. The goal of the presentation is to provide the CEWG with enough information to make a decision without requiring everyone to study the Application for Assessment.

#### **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 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.

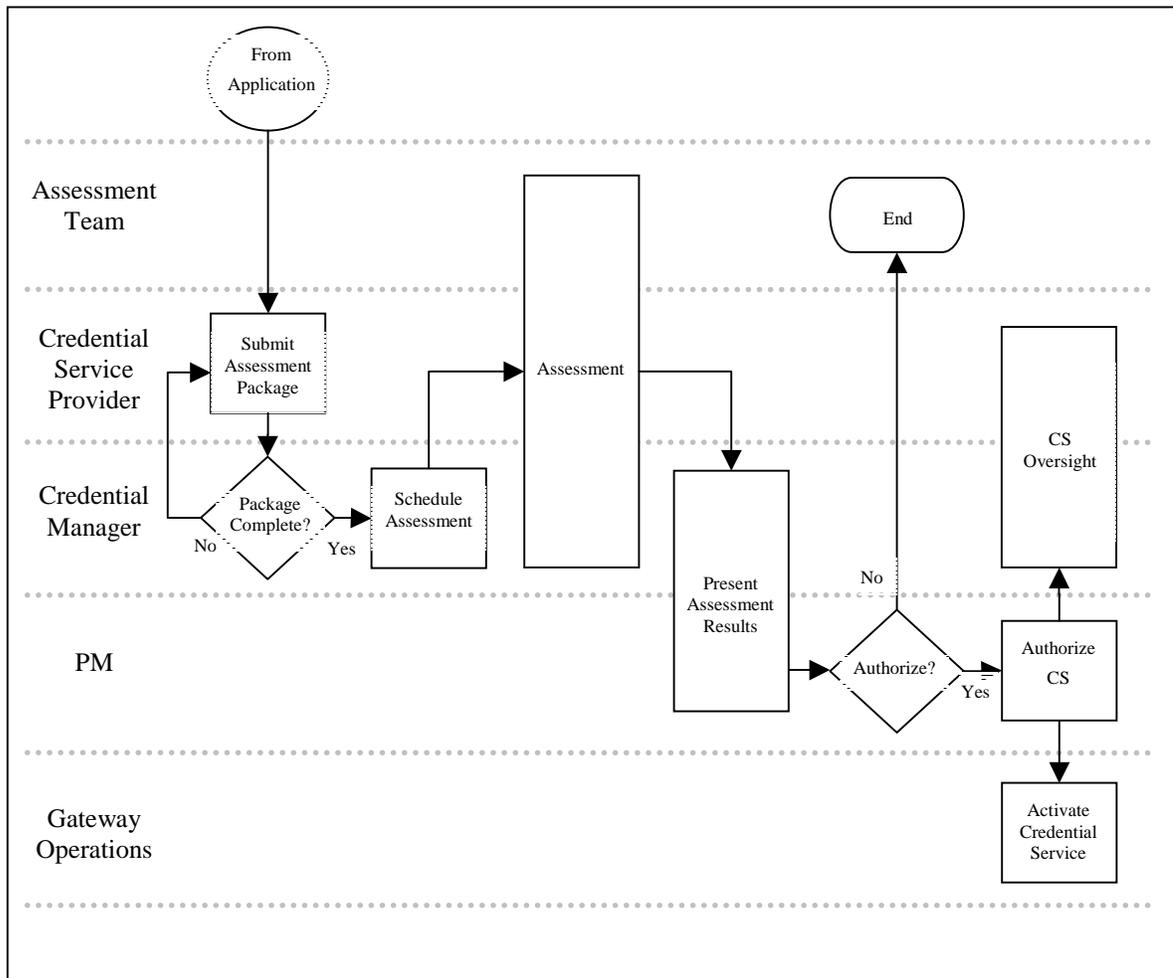
#### **3.1.6 Select Appropriate Credential Assessment Profiles**

CAPs are assigned based on the credential type of the Candidate CSP. The Credential Manager will determine which Profiles are 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 appropriate CAPs 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 the Assessment Package to the Credential Manager. The Assessment Package contains the Evidence of Compliance for each criterion in the applicable Credential Assessment Profiles. The evidence may include results from audits conducted by other parties within one year of package submission.

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, just enough information is required for the Assessment Team to make an informed decision.

Evidence may be provided by the Agency Application (AA) in cases where only a single 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

### **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.

### **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 Credential Assessment Profiles. Conformity 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.

The Credential Manager is not involved in the evaluation of evidence for criteria. The Credential Manager serves in a coordination role. Only Designated 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 for. 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 E-Authentication Service. The Assessment includes interoperability validation according to the latest interface specifications (<http://www.cio.gov/eauthentication/>).

See the Credential Assessment Guidance and the CAP Portfolio for more information.

### **3.2.5 Present Assessment Results**

The Credential Manager will present the final Assessment results 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 exceptions, grant Approval for the CS.

### **3.2.7 Authorize CS**

The PM will provide authorization to operate as a trusted CS through executing a service agreement with the CSP for the authorized 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 PMO of any material changes (i.e., changes the status of evidence from compliant to non-compliant) on the CS that may lower 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. The re-assessment would only cover those elements that have changed.

The PM may require re-assessments if updates to any Credential Assessment Profiles may affect the Assurance Level of the CS. The re-assessments would only cover the criteria that were changed in the profile update.

Annual renewal agreements are required for a CS to remain authorized. 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 level 2 or higher every two years. Other audits may be internal. The PMO may require a partial re-assessment if the scope of the audits does 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 MOU, including maintenance requirements.

### **3.2.9 Activate Credential Service**

Once the CS is authorized to operate, the E-Authentication Service operational team will activate the CS on the E-Authentication Service.

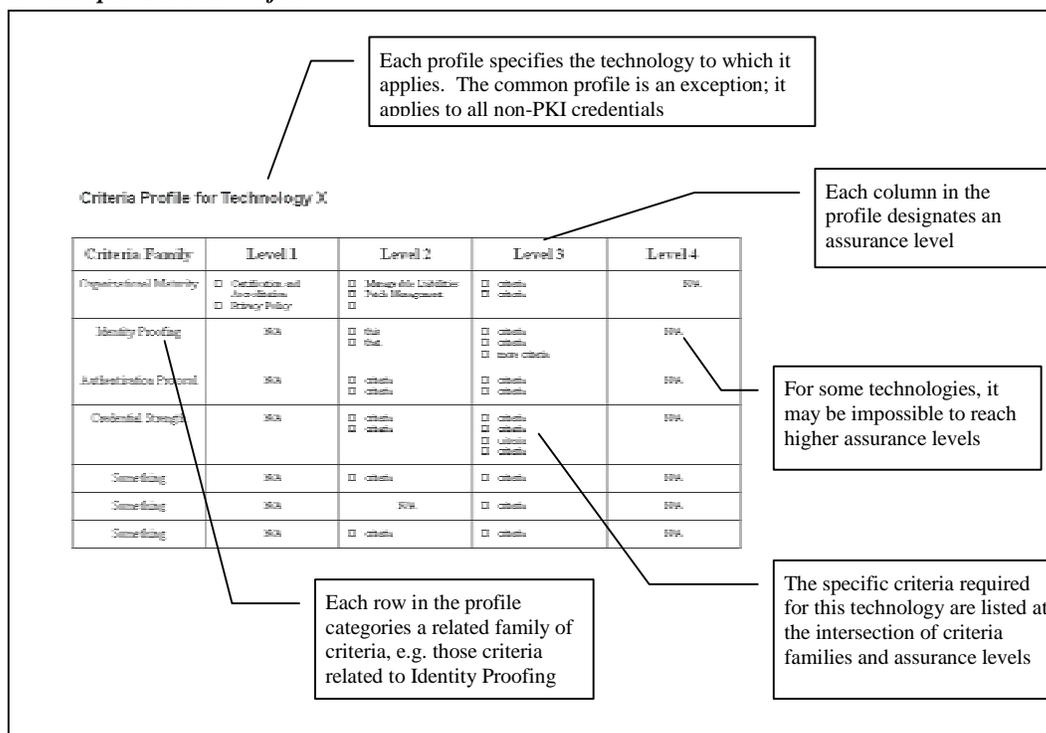
## 4 CREDENTIAL ASSESSMENT PROFILES

### 4.1 Description

The specific requirements for a CS to be assessed at a particular Assurance Level are expressed in Credential Assessment Profiles (CAPs). The E-Authentication initiative will have multiple profiles and is expected to add additional profiles over time. The Common CAP establishes requirements that are standard across any non-PKI CS. Profiles also exist for particular types of CSs, such as Personal Identification Number (PIN) or password-based services. Any non-PKI CS will be assessed against at least two profiles; the Common profile and a profile relevant to their service type. The PKI CAP covers PKI CSs. Additional profiles may be defined over time for types of CSPs, such as banks or Government agencies.

Each individual criterion is named and defined in each profile. The criteria are divided into families of related requirements, such as identity proofing or authentication protocol. The profile also defines which criteria are required for each authentication level. Figure 3 shows an example criteria profile.

Figure 3 Example Criteria Profile



CSPs prepare their submission by providing Evidence of Compliance to satisfy each criterion in applicable profiles. 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 level for which all criteria have been validated, including lower Assurance Levels.

## **4.2 Profile Development**

Technology changes rapidly and authentication technology is no exception. As new technologies become available and show promise for the E-Authentication initiative the PMO will prepare applicable profiles. The CEWG will oversee the preparation of all new profiles.

## **4.3 Profile Maintenance**

The E-Authentication initiative will evolve over time. As the needs of the initiative change or become clearer, it is likely that Criteria Assessment Profiles will evolve. The CEWG has responsibility for profile maintenance. The profiles must be ratified by the ESC before they become effective. As new profiles are being drafted they will be made available to CSPs for comment, and those comments will be provided to the ESC before the profiles are ratified.