



E-Authentication

Interim Credential Assessment Guidance

(CAG)

12/19/2003

release 1.3.0

Executive Summary

This document gives general guidance concerning assessments performed under the US Government's Interim Credential Assessment Framework (CAF). It is intended principally for use by Assessors to ensure assessments are performed consistently, adhere to appropriate policies and conform to applicable standards. Additionally, this document may be used by Credential Service Providers (CSPs) whose services are being assessed and relying parties which require assurance as to the veracity of identity credentials.

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 CAF, CAG, and CAPs (Common, Password, and PIN) currently comprise the CAF suite, which governs the E-Authentication Service initiative. The CAF suite listing is maintained on the E-Authentication website.

Release Notes

Interim Release

Document History

Status	Release	Date	Comment	Audience
Draft	1.0.0	7/10/2003	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">▪ §1.3 Revision to remove references to this specific 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NB - this document supersedes 1.1.0, which was overtaken by release of the Nov. 2003 draft of NIST SP 800-63 and withdrawn before release.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

Editors

Chris Loudon
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	BACKGROUND	1
1.2	PURPOSE.....	1
1.3	TERMINOLOGY.....	1
1.4	DOCUMENT SCOPE.....	2
2	SCOPE OF ASSESSMENTS	3
2.1	CREDENTIAL ASSESSMENT PROFILES	3
2.2	EVIDENCE.....	3
2.3	RELIANCE ON OTHER ASSESSMENT RESULTS	4
2.4	SCOPE OF ASSESSMENTS	4
3	GENERAL ASSESSMENT GUIDANCE	5
3.1	DESIGNATION OF ASSESSORS	5
3.2	RESPONSIBILITIES	5
3.3	QUALIFICATIONS	5
3.4	INDEPENDENCE	5
4	GENERAL GUIDANCE TO DESIGNATED ASSESSORS	7
4.1	PLANNING	7
4.2	COMMUNICATIONS.....	7
4.3	PROFESSIONAL JUDGMENT AND INTERPRETATION	7
4.4	ASSESSMENT CLOSE-OUT	8
5	ASSESSMENT REPORT CONTENTS	8
5.1	ASSESSMENT OBJECTIVE.....	8
5.2	SCOPE AND METHODOLOGY.....	8
5.3	FINDINGS.....	8
5.4	RECOMMENDATIONS.....	9
5.5	DISCLOSURE AND DISTRIBUTION.....	9
6	REFERENCES.....	10

1 INTRODUCTION

1.1 Background

The E-Authentication 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.

Critical to the success of the E-Authentication Initiative is the assessment and approval of Credential Services (CSs). 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. Within the CAF, it is the task of *Designated Assessors* to perform assessments of credential-issuing services against the criteria outlined in the Credential Assessment Profiles at the Assurance Level claimed for the service.

For those CSPs that meet the criteria, the E-Authentication PMO will issue *Authorization to Operate* to the CSP, at the determined Assurance Level.

1.2 Purpose

The purpose of this document is to provide general guidance for conducting assessments performed under the US Government's Interim CAF. It is intended principally for use by Designated Assessors to ensure that: assessments are performed consistently and professionally; pertinent government policies and regulations are recognized and considered by Assessment Teams; and Assessment Reports are accurate, complete and useful to the E-Authentication PMO in their final evaluation of the CSP.

This document also may be used by CSPs whose services are being assessed and relying parties that will use the Credential Service (CS). This document alerts these organizations as to the qualifications of assessors, how they should expect an Assessor to perform assessments, interpret criteria and make professional judgements regarding evidence.

1.3 Terminology

This document relies upon terminology established in the E-Authentication Interim CAF, with which the reader is assumed to be familiar.

1.4 Document Scope

This document is limited to providing general guidance to Designated Assessors and CSPs, it is not a 'how to' guide for Assessments. It is expected that Assessors will use this document and other CAF materials as the basis and structure for applying their professional judgment.

This document does not contain specific assessment criteria. The CAF is a modular framework in which specific Assessment Profiles that contain the specific assessment criteria are developed and used appropriately. The guidance contained in the document is 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'.

2 SCOPE OF ASSESSMENTS

2.1 Credential Assessment Profiles

The scope of each assessment is bound by the criteria contained in the Credential Assessment Profiles (see description in Section 4 of the Credential Assessment Framework document). Based on the Credential Service offered, Profiles for assessment are assigned to CSPs. Using the criteria in the selected Profiles, the Designated Assessor is expected to evaluate and assess evidence relating to a CSP's general business practices, security and internal controls. Generally, each criterion of the Profiles 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.

2.2 Evidence

By completing the Assessment Package, CSPs assert their compliance with Profile criteria. Evidence could be in the form of an audit report or certificates from other external/independent assessments. It may be necessary to work with the Designated Assessor to develop a mutually acceptable list of evidence sufficient for the assessor 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, Designated Assessors shall form a judgement of the status and

determine if the E-Authentication Initiative recognizes the competence of the previous Assessor.

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. In the event that a CS is authorized under this stipulation, that authorization shall be rendered invalid should the CS be put into use by any additional AA(s).

2.3 Reliance on other Assessment Results

A fundamental premise of the CAF is that CSPs (in particular Level 2 and above) have likely undergone similar assessments (e.g. SAS 70, ISO 17799, WebTrust for CAs, etc.) 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 Assessor 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 Level 1 Credential Services may need not have undergone other assessments or audits.

The CAF, through its Credential Assessment Profiles, cites specific standards which are required to be fulfilled in order to satisfy criteria. The CAF itself does not establish standards *per se*, but establishes criteria which have to be satisfied by the provision of evidence, which might include proof of compliance with pertinent standards or successful completion of an audit.

2.4 Scope of Assessments

The Assessment process begins only after the E-Authentication Project Management Office (PMO) has made the decision to accept the application from the CSP. As described in CAF Section 3.1, Application for Assessment, the E-Authentication PMO will make a determination on the suitability and financial viability of an applicant CSP in making the decisions to accept the CSP application and recommend that an assessment is warranted.

3 GENERAL ASSESSMENT GUIDANCE

3.1 Designation of Assessors

Assessors are designated by the Program Management Office (PMO) based on qualifications criteria.

Designation of Assessors is solely the responsibility of the Project Manager (PM). The CEWG will recommend to the PM criteria for Assessor designation that will include their required qualifications. The PM will make the final criteria determination, and will maintain a list of active and approved Designated Assessors.

3.2 Responsibilities

The CAF places assessment-related responsibilities on the PMO and Assessors.

The PMO is responsible for maintaining and updating this document, ensuring that assessments are conducted by Designated Assessors personnel who have the necessary skills, and that independence is maintained. The Designated Assessor is responsible for ensuring that the practices and processes prescribed in the CAF are followed in planning and conducting assessments as well as preparing Assessment Reports. The PMO is responsible for reviewing Assessment Reports and issuing Authorization to Operate.

3.3 Qualifications

The selected Assessment Team shall collectively possess adequate technical proficiency and industry knowledge for the specific Assessment being performed.

The PMO has the responsibility to ensure that each Assessment is conducted by staff that collectively have the knowledge and skills necessary for a specific Assessment. The team should have a thorough knowledge of the government's E-Authentication requirements, understanding of the CSP's industry and expertise in the specific technologies/techniques being assessed.

3.4 Independence

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 judgements and recommendations will be impartial. If any circumstance affects an Assessor's ability to perform the Assessment and report findings impartially, that Assessor should decline to perform the Assessment.

Designated Assessors may be required to sign Non-Disclosure Agreements with the CSP or declare any potential conflicts of interests relating to an assessment.

4 GENERAL GUIDANCE TO DESIGNATED ASSESSORS

4.1 Planning

Assessments are to be adequately planned.

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

4.2 Communications

Establish and maintain communication with the designated management of the CSP.

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

4.3 Professional Judgment and Interpretation

Assessors are required to exercise a degree of subjective judgement when applying criteria to various CSPs.

Despite the structure of the CAF and its associated Profiles, Designated Assessors will have to rely on their experience and domain knowledge when determining a CSP's conformity to specific criteria. However to ensure that Assessments are conducted consistently, the CEWG reviews the criteria adopted in the CAPs. 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 CS. 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.

4.4 Assessment Close-Out

The Assessor 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 Assessor 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.

5 ASSESSMENT REPORT CONTENTS

The Assessor must prepare a written Assessment Report to document the approach, findings, and its recommendation re. authorisation of the CS. The Assessment Report must include:

- Assessment Objective;
- Scope and Methodology;
- Findings; and
- Authorization recommendation (including Level of Assurance).

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

5.1 Assessment Objective

The Assessor should identify the CSP and state the identity of the CS being offered.

5.2 Scope and Methodology

Based on the Assessment Objective, the Assessor should identify the Credential Assessment Profiles applicable to the CS, the sources of evidence and period of the Assessment. The Assessor should define the type of credential that is being offered, the claimed level of Assurance and explain the current use of the credential (online banking, Internet Service Provider, etc).

5.3 Findings

The Assessor should report the CSP's compliance with the criteria contained in the assigned Credential Assessment Profiles. For each criterion, the Assessor should identify the evidence provided, rational for acceptance or rejection and any deficiencies identified.

5.4 Recommendations

Based on the scope and results of the Assessment, the Assessor must provide the E-Authentication PM with a recommendation for authorisation or rejection of the application, including their determination as to what Level of Assurance any authorisation should be granted.

5.5 Disclosure and Distribution

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 to other parties for any reason.

6 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] “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)