Certificate Life-Cycle Methodology
and
Criteria

For the

United States
E-Governance Certificate Authorities

Prepared By:
The E-Authentication Program Management Office

Version 4.0: January 12, 2005
FINAL DRAFT

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Objective

This document outlines the methodology and criteria for the issuance and management of certificates from the United States Government's e-Governance Certificate Authorities (E-GCAs).

1.2 Intended Audience

This document is intended for information technology officials, PKI managers, and personnel involved in Credential Service Providers (CSPs) and Agency Applications (AAs) activities within the government and between government and external entities.

1.3 Background

As part of the President's Management Agenda, the E-Authentication initiative has been established to enable trust and confidence in E-Government transactions via the establishment of an integrated policy and technical infrastructure for electronic authentication. The result is the Authentication Service Component (ASC).

The ASC is a federated architecture including users, AAs, and CSPs, which leverages credentials from multiple domains through certifications, guidelines, standard adoption and policies.

The architecture provides the ability for AAs and CSPs to operate at assertion-based authentication assurance levels (e.g., pin and passwords) by obtaining Transport Layer Security (TLS) server certificates from the e-Authentication Governance Certificate Authorities (E-GCAs). These server certificates are issued from the Federal Public Key Infrastructure Architecture (FPKIA) to secure the Simple Object Access Protocol (SOAP) connection used to transport the identity assertion between AAs and CSPs.

1.4 Governance

The Federal Public Key Infrastructure Policy Authority (FPKIPA) has governance of the operations of the E-GCAS. However, the issuance and management of the E-GCAs certificates have been delegated to the E-Authentication Authorizing Official (EAO).

The FPKIPA has authorized the FPKI Operational Authority (FPKI OA) to establish three (3) E-GCAs. The FPKI OA will issue TLS server certificates to approved CSPs at levels one (1) and two (2) and to AAs. These certificates will satisfy a cryptographic binding between the authentication and transaction requirement, which is available using client certificates over TLS protocols, as described in the e-Authentication Technical Approach document at http://www.cio.gov/eauthentication/TechSuite.htm.

The EAO will authorize the FPKI OA to issue E-GCAs certificates, as well as, perform other certificate management activities throughout the certificate life cycle.

2.0 CERTIFICATE ISSUANCE PROCESS

A request for an E-GCA certificate triggers a multi-phase process designed to achieve a mutually reliable trust relationship. Figure 1-1 depicts this process.

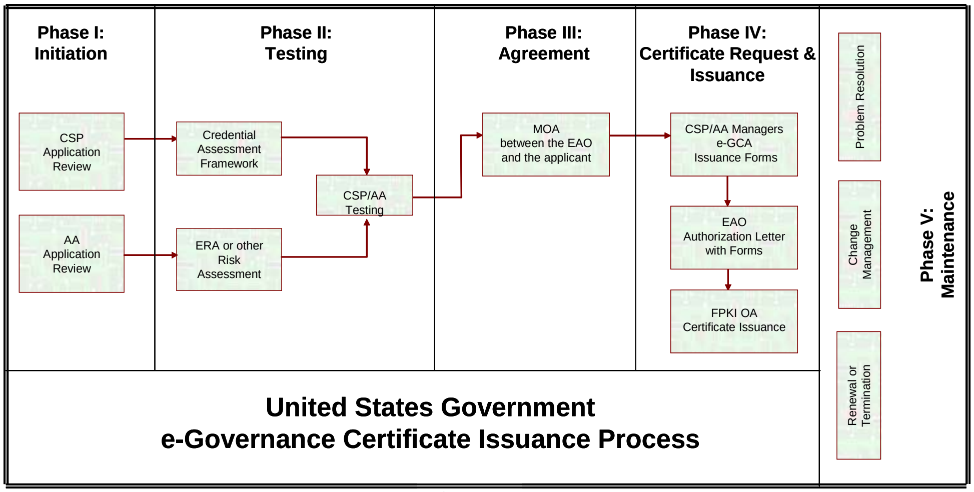
Phase I: Initiation
CSP Application Review
AA Application Review
Phase II: Testing
Credential Assessment Framework
ERA or other Risk Assessment
CSP/AA Testing
Phase III: Agreement
MOA between the EAO and the applicant
Phase IV: Certificate Request & Issuance
CSP/AA Managers e-GCA Issuance Forms
EAO Authorization Letter with Forms
FPKI OA Certificate Issuance
Problem Resolution
Change Management
Renewal or Termination
Phase V: Maintenance
United States Government
e-Governance Certificate Issuance Process

Figure 1-1

2.1 Phase I – Initiation

Purpose: To prepare and submit the required information to receive a certificate from an E-GCA.

Activities:

The Applicant contacts the EAO to initiate the process to participate in the e-Authentication architecture. A preliminary discussion will be held to determine the applicant’s suitability and readiness to pursue the process.

The EAO directs the Applicant (i.e., CSP or AA) to the website where the documents can be found to assist in becoming an E-Authentication customer:

1) PKI Application
   www.cio.gov/eauthentication/PKI Application.doc
2) E-GCA Certificate Server Request Form
   www.cio.gov/eauthentication/E-GCA Certificate Server Request Form.doc
3) E-Governance Certificate Authorities Technical Guidance
   www.cio.gov/eauthentication/E-GCA Technical Guidance.doc

4) The Certificate Life-Cycle Methodology & Criteria for the U.S. E-Governance Certificate Authorities
   www.cio.gov/eauthentication/E-GCAs Methodology & Criteria.doc
5) X.509 Certificate Policy for the E-Governance Certificate Authorities
   http://www.cio.gov/fpkipa/documents/EGovCA-CP.doc
6) Customer Support
   http://www.cio.gov/eauthentication/Customer Support.doc

The Applicant completes an application available on the e-Authentication website. Upon completion, the Applicant is assigned a CSP or AA manager. The Applicant may seek assistance from his or her CSP or AA manager in completing or revising the application, which seeks the following information:

(a) Applicant identifying information and contacts;
(b) Reason for requesting an E-GCA certificate;
(c) A description of the Applicant's proposed technical operational environment and configuration, and clients; and
(d) The proposed credential (i.e., CSP level 1, CSP level 2, and AA) sought.

The Applicant submits the completed application (which has been signed by the appropriate senior officials) to the EAO. The Applicant's certificate issuance request form(s) may be submitted during phase three (3) of the certificate issuance process, as depicted in Figure 1-1.

Submission should be made in both writing (hardcopy/wet signature) and accompanied by an electronic copy (.doc, .rtf) of their application.

2.2 Phase II – Testing

Purpose: The E-Authentication Initiative has designated the e-Authentication Lab for the purpose of identifying and resolving potential technical issues and to minimize the risk of introducing incompatibilities with existing affiliates.

Activities:

- **Credential Assessment Framework**

  The E-Authentication Initiative maintains a Trust List, which contains the Credential Services (CSs) that can be used by the initiative. Credential Service Providers (CSPs) are assessed using the Credential Assessment Framework (CAF). 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 EAO which makes the final decisions on additions to the Trust List. More information is available at http://www.cio.gov/eauthentication/CredSuite.htm.

- **Risk Assessment**

  All AAs participating in the E-Authentication architecture must undergo a risk assessment to identify the risks associated with insufficient authentication of users, and to form the basis for the definition of authentication requirements.

  The E-Authentication Initiative teamed with the Software Engineering Institute (SEI) at Carnegie Mellon University to develop a risk-based approach to authentication requirements, called the **E**lectronic **R**isk and **R**equirements **A**ssessment, or **E-RA**. It identifies the risks associated with insufficient authentication of users, and it forms the basis for the definition of authentication requirements. It is available for all AAs at no cost at http://www.cio.gov/eauthentication/era.htm.

- **Interoperability Testing**

  The assigned CSP or AA manager contacts the Applicant to organize an initial meeting to allow the E-Authentication Technical Team or technical lead to meet with key persons, discuss the application, architecture, and technical testing process.

  Having shared their respective information, the Applicant and the E-Authentication Technical Team undertake a test. The tests will follow a formal test process in order to determine if secure business transactions can be conducted within the E-Authentication architecture and between approved CSPs and AAs. In addition, the testing process will:

  (a) Determine the configuration and if it is compliant with the E-Governance Certificate Policy requirements;
  (b) Permit the making of a decision to proceed, proceed with conditions, terminate or re-schedule tests throughout the test; and
  (c) Document detailed test results.

  The E-Authentication Technical Team reports the findings of the test in the Analysis of the Applicant Demonstrations Report to the assigned CSP or AA manager for review and direction.

  The assigned CSP or AA manager will provide directions in one of the following ways:

  (a) Proceed to the next step without conditions;
  (b) Proceed to the next step, with acceptance by EAO conditions; or
  (c) Terminate process.

If the decision is to proceed, then the EAO establishes a Memorandum of Agreement (MOA) with the Applicant and schedules a date for certificate issuance from the E-GCA operational environment. Otherwise, the process is terminated and the EAO notifies the Applicant point-of-contact.

2.3 Phase III – Agreement

Purpose: To negotiate the terms and conditions of the MOA.

Activities:

1. In consultation with legal counsel, the EAO determines which type of document is appropriate to serve as the template for a MOA. Minimally, there will be at least three different template documents: an external MOA for an external Applicant, an interdepartmental MOA for a Federal department or agency, and some other formal arrangement, such as a treaty with a foreign government.

2. Process for External MOA

   a) The EAO provides a review copy of the appropriate draft arrangement to the Applicant's contact.
   b) The EAO provides any additional information or clarification required by the Applicant.
   c) The EAO and the Applicant negotiate text for the proposed agreement.

3. Process for Interdepartmental MOA

   a) The EAO provides a review copy of the MOA to the Applicant's contact.
   b) The EAO provides any additional information or clarification required by the Applicant.
   c) The EAO and the Applicant negotiate text for the proposed agreement.

4. Common Activity: Negotiation

   a) The EAO may review any relevant documentation, such as subscriber or service provider agreements, related to the Applicant operation.
   b) Areas of disagreement are reviewed and resolved.
   c) The EAO is the signatory for the E-Authentication Initiative
   d) The Applicant must designate a cognizant Authority to be its signatory.

2.4 Phase IV – Certificate Request and Issuance

Purpose: To initiate the process allowing the FPKI OA Team to issue an E-GCA certificate.

Activities:

Each CSP or AA requiring an E-GCA certificate must complete an E-GCA Server Certificate Request form. If a single server will host multiple CSs or AAs, a separate form is required for each request.

Below are the required fields that must be completed. Confirmation of the information contained in the form may be requested.

E-GCA Server Certificate Request Form

All Information Required

General Information	
Request Date:	*EX: July 16, 2004*
Agency:	*EXAMPLE AGENCY*
E-Authentication Point of Contact:	*JOHN DOE; john.doe@example.gov*
Agency Point of Contact:	*JANE DOE; jane.doe@example.gov*
Request Reason:	*Initial Request; Expired Cert; Replace a Revoked Cert, etc*

Application Information	
Application Name:	*EX: SAMPLE CS, SAMPLE AA*
Authentication Assurance Level:	*CSP Level 1, CSP Level 2 or AA ONLY*

Server Information	
Server Hostname:	*Ex: CS.SAMPLE-ORG.COM, AA.SAMPLE-AGENCY.GOV*
Server IP Address:	*EX: 255.255.255.255*

The EAO signs the certificate issuance authorization letter for the assigned CSP or AA manager.

The CSP or AA manager receives and sends the PKI application, E-GCA certificate request form(s) and the E-Gov certificate issuance authorization letter from the applicant and EAO respectively, to the FPKI OA Program Manager.

FPKI OA Team reviews the form(s) and letter.

Following a satisfactory review of the technical data, the FPKI OA Team takes the necessary procedural and technical steps to issue a certificate, to include a PEM or DER encoded PKCS#10 self-signed certificate request from the applicant. See E-Governance Technical Guidance document for technical steps.

Upon an Applicant receiving an E-GCA certificate they are considered an Affiliate of the e-Authentication Architecture.

Upon request (via the authorization letter), the FPKI OA can publish the issued certificates to the FPKI directory using the *userCertificate* attribute under the DN of the issuing CA (i.e. certificates issued by the CA with DN 'ou=eGovCSP1,ou=FBCA,o=u.s. government,c=us' would be posted at the 'ou=eGovCSP1,ou=FBCA,o=u.s. government,c=us' level).

2.5 Phase V – Maintenance

Purpose: To provide mechanisms both for managing the relationship between the affiliate and the EAO as required for the proper operation of the arrangement, and for terminating the arrangement if either party contravenes its terms and conditions. The elements of this phase are not sequential and they will apply as circumstances warrant.

Activities:

- Compliance Review
- Problem Resolution
- Change Management
- Renewal or Termination

It is important to ensure that, once in place and for its duration, the arrangement continues to guarantee the agreed upon level of trust between the EAO and the Affiliate.

The maintenance phase provides mechanisms both for managing the relationship between the two entities as required for the proper operation of the arrangement, and for terminating the arrangement if either party contravenes its terms and conditions or at the desire of either party. The elements of this phase are not sequential and they will apply as circumstances warrant.

- **Compliance Review**

Purpose: In the event of a concern, to determine if the Affiliate is operating in compliance with the X.509 Certificate Policy for the U.S. E-Governance Certificate Authorities and
MOA practices.

The E-Authentication Technical Team may raise concerns about an Affiliate to the assigned CSP or AA manager.

The assigned CSP or AA manager contacts the Affiliate for information and to ensure that it is in compliance with the X.509 Certificate Policy for the U.S. E-Governance Certificate Authorities and MOA practices.

The CSP or AA manager will notify the E-Authentication Technical Team and the FPKI OA Program Manger in the following ways:

(a) Indicate no problem exists and recommend continuation of the affiliation unchanged;
(b) Indicate any deficiencies and suggest correct action, but recommend that the Affiliate continues to operate at its current assurance level;
(c) Recommend renewal, but further recommend that the EAO downgrade the assurance level of the certificate; or
(d) Recommend that the EAO revoke the certificate.

- **Problem Resolution**

Purpose: To report and correct problems the parties may encounter during the effective period of the agreement.

Either party to the arrangement may notify the other of problems and request resolution. Problem resolution procedures are specific to the problem encountered and will be agreed upon between the parties.

- **Change Management**

Purpose: To manage changes to the Federal Public Key Infrastructure Architecture (FPKIA) or Affiliate system associated with a particular agreement and to decide what actions to take as a result of implementing such changes.

Either party to the agreement may initiate this process. If either the FPKIA or Affiliate system is contemplating changes that impact the terms of the agreement, then a notice of the change must be provided to the other party.

Each party reviews the notice and determines the appropriate response:

a. Unconditional acceptance of the proposed change(s);
b. Conditional acceptance, with follow-up required; or
c. The change is found to be unacceptable.

If a change implemented by one of the parties is deemed unacceptable to the other, such implementation may cause termination of the agreement.

Renewal or Termination

Purpose: To decide whether to renew or terminate an existing arrangement, and to specify the process for either renewal or termination.

Should the FPKIPA, the FPKI OA, or the EAO become aware of any information that indicates that there has been a failure in the integrity of the Affiliated System that is deemed by any of the Entities to have the potential to adversely affect the security of the FPKIA and its other affiliates, then the EAO, at his or her discretion, may instruct the FPKI OA to revoke the certificate of the Affiliated System. The EAO informs the Affiliate point-of-contact of the revocation.

APPENDIX A. Sample E-Governance Certificate Issuance Authorization Letter

Date: (Date of writing this letter)

Memorandum For: (Name of Federal PKI Operational Authority Program Manager)
(Title)
(Office)

From: (Name of E-Authentication Authorizing Official)
(Title)
(Office)

Subject: Authorization to Issue E-Governance Certificates

The (Applicant name) has been successfully added to our trust list as the following:

[CSP Level 1, CSP Level 2, Agency Application]

The (Applicant name) has provided the e-Authentication Authorizing Official with the X.500 distinguished name of the application and additional extensions that is requesting certification issuance from the E-Governance Certificate Authority (CA).

Example: [c=US; o=(Organization); ou=(Entity name); ou=(Entity distinguished name) ;
cn=(DNS Name)]]

Additional Extensions:
SubjectAltName: [email address of contact]

The (Applicant name) [has, has not] requested that their certificate be published to the FPKIA directory.

The (Applicant name) has provided the EAO with the following information via official channels.

Applicant Mailing Address:

Name of Applicant's Authorizing Official:
Email address:
Phone number:

Program Manager POC name:
Program Manager POC telephone number:
Program Manager POC email address:

Primary Technical POC name:
Primary Technical POC telephone number:
Primary Technical POC email address:

Alternate Technical POC name:
Alternate Technical POC telephone number:
Alternate Technical POC email address:

APPENDIX B. Sample E-Governance Certificate Revocation Authorization Letter

Date: (Date of writing this letter)

Memorandum For: (Name of Federal PKI Operational Authority Program Manager)
(Title)
(Office)

From: (Name of E-Authentication Authorizing Official)
(Title)
(Office)

Subject: Authorization to Revoke E-Governance Certificates

The (Affiliate name) has been removed from our trust list. The certificate should be revoked for the following reason: