FINAL DRAFT

E-Governance Certificate Authorities Technical Guidance

January 12, 2005

Table of Contents

1. Background

The E-Authentication Initiative has established E-Governance Certificate Authorities (E-GCAs), as part of the Federal Public Key Infrastructure Architecture (FPKIA).

There are a total of three (3) E-GCAs. Two (2) are assigned to issue certificates for Credential Service Providers (CSPs) at e-Authentication levels "one" and "two" and one (1) to issue certificates to Agency Applications (AAs).

These certificates are required to secure the Simple Object Access Protocol (SOAP) channel used to pass the identity assertion between CSP and AA in the E-Authentication Federated Architecture.

2. Scope

The scope of this document is to provide general technical information that will assist in generating certificate signing requests for E-GCA certificates.

It also provides an overview of the process of how to obtain each type of E-GCA certificate offered by the E-Authentication Initiative.

3. General Technical Information

To obtain a certificate, an applicant must submit a PKCS#10 (RFC 2986) in accordance with the E-Governance profile described in section 7.1 of the X.509 Certificate Policy for the E-Governance Certification Authorities.

The PKCS#10 should contain a subject DN, the public key and any other optional extension information. The PKCS#10 should also be signed. Additional extensions, such as Certificate Revocation List (CRL), Certificate Policies and Authority Information Access (AIA) will be added to the certificate at the time off issuance.

The PKCS#10 should contain the subject name as described in section 7.1.4 [CP-eGov]. It should also be signed using a 2048 bit key using Sha1 with RSA Encryption (1.2.840.113549.1.1.5) or Sha256 with RSA Encryption (1.2.840.113549.1.1.11), as described in section 7.1.3 [CP-eGov].

Some CAs do not produce properly formatted PKCS#10 certificate signing requests. In this case, a PKCS#10 request must be manually generated.

Sections below describe details about the issuance process for each type of certificate for the E-Authentication Initiative.

4. E-GCA Test Certificates

Applicants must contact 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.

Most agencies applications participating in the E-Authentication Initiative are proof-of-concepts and require test certificates to identify and resolve potential technical issues.

Test certificates are issued to an applicant from the Prototype FPKIA upon request from a Credential Service Provider or Agency Application Manager via e-mail. These managers may delegate a request through a technical team.

To ensure proper work flow, an authorized applicant can directly contact the Federal Public Key Infrastructure (FPKI) Operational Authority (OA) Technical Lead [andrew.lins@mitretek.org] to request a certificate and to discuss technical details (e.g., what extensions to include in the certificate, what type of certificate is to be issued, whether the certificate should be issued from the E-GCA CSP1, CSP2, or AA).

Once all of the technical details have been discussed, the E-Authentication team member submits a PKCS#10 certificate request (as described in Section 3.0, General Technical Information) to the Technical Lead via e-mail.

The Technical Lead signs the certificate and sends it back to the authorized entity via e-mail.

5. Agency Application Certificates

Agency Application certificates are issued from the Production FPKIA to applications that have undergone risk assessments and are operating in production environments.

Agency Application Certificates are only issued to agencies authorized by the E-Authentication Authorizing Official through memorandum as described in Section 2.4 of the Certificate Life-Cycle Methodology and Criteria for the U.S. E-Governance Certificate Authorities.

Authorized applicants submit PKCS#10 certificate requests, as described in Section 3.0, General Technical Information, via agreed upon out-of-band mechanisms (courier, in-person, etc).

6. Credential Service Provider Certificates

CSP certificates are issued from the Production FPKIA to CSPs that have undergone credential assessments and are operating in production environments.

CSP certificates are only issued to CSPs that are authorized by the E-Authentication Authorizing Official through memorandum as described in Section 2.4 of the Certificate Life-Cycle Methodology and Criteria for the U.S. E-Governance Certificate Authorities.

Authorized applicants submit PKCS#10 certificate requests, as described in Section 3.0, General Technical Information, via agreed upon out-of-band mechanisms (courier, in-person, etc).

7. REFERNCES

The following documents are referenced in this document:

1. X.509 Certificate Policy for the E-Governance Certification Authorities website: [http://www.cio.gov/fpkipa/documents/EGovCA-CP.doc].

2. Certificate Life-Cycle Methodology & Criteria for the U.S. E-Governance Certificate Authorities website: www.cio.gov/eauthentication/E-GCAs Methodology & Criteria.doc