Citizen & Commerce Certificate Policy Version 1.0, December 3, 2002

1. Introduction

This Certificate Policy defines requirements for certificates accepted by the U.S. Federal Government for the purpose of authenticating citizens and commercial enterprises for many electronic services. There are two levels of assurance defined by this policy: a provisional policy where assurance is based on vendor declaration for six months; and an approved policy where assurance is based on policy mapping and review by the FPKI Policy Authority's Certificate Policy Working Group.

This policy is identified by the following OIDs:

citizen-and-commerce-provisional ::= 2.16.840.1.101.3.2.1.14.1
citizen-and-commerce-approved ::= 2.16.840.1.101.3.2.1.14.2

These policy OIDs may be asserted by the U.S. Federal Government in CA certificates issued to certificate providers whose policies satisfy these requirements and issue certificates to citizens and commercial entities. The citizen-and-commerce-provisional OID indicates that the certificate provider stipulates that they satisfy all requirements of this CP. The citizen-and-commerce-approved OID indicates that the Federal PKI Policy Authority, or its agent, has reviewed the provider's policy and determined that it meets the requirements for this policy.

The Federal PKI Policy Authority is responsible for all aspects of this CP. Questions regarding this CP shall be directed to the Chair of the Federal PKI Policy Authority, whose address can be found at http://www.cio.gov/fpkipa.

2. GENERAL PROVISIONS

This policy requires CAs to issue certificates, maintain and distribute certificate status information, and protect the private key(s) used to sign certificates and certificate status information.

This policy requires subscribers to inform the CA if they believe their private key(s) have been compromised, stolen, or lost.

Relying parties determine whether or not certificates that satisfy this policy are appropriate for their application, and whether certificate status information need be verified before use.

2.1 Liability

Transactions involving private citizens, businesses and government agencies are controlled by state, local and federal law. The Federal Tort Claims act defines the circumstances under which a federal agency may be held liable for the negligent acts of one (or more) of its employees. Negligent acts committed by businesses and individuals will be controlled by state and local law.

2.2 Financial responsibility

This CP contains no limits on the use of its certificates. Limits on financial liability should be established by the CA in advance of use of Certificates issued under this policy. In the absence of any such agreement, a financial limit of $500.00 is presumed.

2.2.1 Indemnification by relying parties

Under no circumstances will a federal agency agree to indemnify a CA issuing certificates under this policy. CAs and subscribers may reach their own agreements as to indemnification.

2.2.2 Fiduciary relationships

Federal agencies agreeing to use these certificates do not have a fiduciary relationship with CAs operating under this policy. The existence of a fiduciary relationship (if any) between CAs and subscribers is determined by contract or agreement between those parties.

2.2.3 Administrative processes

Processes (if any) shall be agreed upon between the FBCA and the CA and memorialized in an agreement.

2.3 Interpretation and Enforcement

2.3.1 Governing law

This CP shall be interpreted under the principles used in construing federal agreements, grants and contracts as interpreted by the U.S. Court of Appeals for the Federal Circuit.

2.3.2 Severability, survival, merger, notice

Should it be determined that one section of this CP is incorrect or invalid, the other section of this CP shall remain in effect until the CP is updated.

2.3.3 Dispute resolution procedures

No stipulation

2.4 Compliance audit

This policy requires successful compliance audit prior to applying for provisional or approved status. The compliance auditor must be organizationally independent from the owner of the CA and qualified to audit CA processes. To maintain approved status, a CA must repeat the compliance audit process at least every three years.

2.5 Confidentiality

Confidentiality requirements (if any) are determined by agreement between subscriber and CA.

3. IDENTIFICATION AND AUTHENTICATION

The CA is responsible for authenticating the identity of the subject before certificate issuance. The identity of the subject must be stated in the common name attribute of the subject distinguished name. The identity may be established in any of the following manners:

(1) The identity may be established through in-person appearance at the credential provider, or its agent, with physical credentials (e.g., driver's license or birth certificate). Collection of certified mail is one example of in-person appearance at an agent of the credential provider.

(2) The identity may be established using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as:
- the ability to place calls from or receive phone calls at a given number; or
- the ability to obtain mail sent to a known physical address.

(3) Where an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, or retail company) exists, the identity may be authenticated through information derived from the business relationship such as:
- the ability to obtain mail at the billing address used in the business relationship; or
- verification of information established in previous transactions (e.g., previous order number) ; or
- the ability to place calls from or receive phone calls at a phone number used in previous business transactions.

The CA is responsible for ensuring the uniqueness of certificate subject names for all certificates issued by that CA. Under no circumstances shall additional certificates containing the same subject name be issued to a different subscriber (person, role, or organization).

When a request to revoke a certificate is received, the CA is responsible for authenticating the identity of the requester.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

CAs that wish to cross certify with the federal Government under this policy shall follow the process described on http://www.cio.gov/fpkipa/index.htm

This policy makes no stipulation regarding certificate application procedures for end entities.

4.2 Certificate Issuance

No stipulation.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

This policy requires CAs to maintain and distribute certificate status information until certificate expiration. When a certificate's status changes, the new status must be available to relying parties within 72 hours.

Certificate status information must be distributed using at least one of the following mechanisms: X.509 CRLs; or the Online Certificate Status Protocol (OCSP). If a certificate is not covered by an X.509 CRL, the certificate must explicitly specify the authoritative OCSP server using the Authority Information Access extension.

4.5 Security Audit Procedures

The CA shall take adequate measures to ensure the security of their operations.

4.6 Records Archival

No Stipulation.

4.7 Key changeover

No stipulation.

4.8 Compromise and Disaster Recovery

No stipulation.

4.9 CA Termination

CA shall inform the FBCA prior to planned termination or suspension of operations. If operations are disrupted by disaster or other unexpected events, notice should be provided shortly thereafter.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

The CA shall take adequate measures to ensure the security of their operations.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

CA and subscriber RSA or DSA private keys must be 1024 bits or larger.

The CA private key(s) used to sign certificates and certificate status information shall be generated in cryptographic modules validated against FIPS 140 Level 2 (or higher). This policy makes no stipulation regarding the generation of subscriber private keys.

End Entity certificates issued under this policy are not required to include the key usage extension; if it appears, the digitalSignature bit must be asserted.

CA Certificates issued under this policy are required to include the key usage extension. Certificates containing CA public keys that are used to verify certificates shall assert keyCertSign; certificates containing CA public keys that are used to verify CRLs shall assert crlSign.

This policy makes no stipulation regarding private or public key delivery, public key parameters generation, or parameter quality checking.

6.2 Private Key Protection

The CA private key(s) used to sign certificates and certificate status information shall be maintained in cryptographic modules validated against FIPS 140 Level 2 (or higher).

This policy makes no stipulation regarding the protection of subscriber private keys.

6.3 Other Aspects of Key Pair Management

No stipulation.

6.4 Activation Data

No stipulation.

6.5 Computer Security Controls

No stipulation.

6.6 Life Cycle Technical Controls

No stipulation.

6.7 Network Security Controls

No stipulation.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7. CERTIFICATE AND CRL PROFILES

This policy requires issuance of X.509 version 3 certificates. Certificates may contain RSA or DSA public keys of 1024 bits or larger. Certificates must be signed using RSA or DSA, with Secure Hash Algorithm version 1 (SHA-1).

CAs that use CRLs to distribute shall distribute X.509 version 2 CRLs.

8. SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

The Federal PKI Policy Authority shall review this CP at least once every year.

8.2 Publication and notification policies

This CP and any subsequent changes shall be made publicly available within one week of approval.

8.3 CPS approval procedures

The CPS for the FBCA CA(s) that issue CA certificates under this policy shall be contained in a separate document approved by the Federal PKI Policy Authority.