



E-Governance CA Certificate Policy Change Proposal Number: 2010-01

To: Federal PKI Policy Authority
From: Certificate Policy Working Group
Subject: Proposed modifications to the X.509 Certificate Policy for the E-Governance Certification Authorities (EGCA CP)
Date: August 5, 2010
Title: Changes to bring the EGCA CP into alignment with recent operational changes to the FBCA CP.

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the E-Governance Certification Authorities – Version 1.4, August 16, 2007.

Change Advocate’s Contact Information:

Name: Cheryl Jenkins
Organization: GSA – FPKI MA
Telephone number: 202-577-1441
E-mail address: Cheryl.Jenkins@gsa.gov

Organization requesting change: Federal PKI Management Authority

Change summary: Bring the EGCA into operational alignment with the FBCA. Specifically:

- Clarify the purpose of archiving, and the archiving requirements for auditable events. Also, clarify that NARA and/or other applicable regulations apply.
- Permit remote administration of the E-Governance Certification Authorities (EGCA) and associated repositories by the appropriate Trusted Roles, so that EGCA Certificate Policy (CP) operational and security requirements are maintained.
- Permit the compliance audit against the full CPS to be conducted over three years as long as some of the key controls are examined annually.

Background: In 2008, the FPKIPA adopted a change to the FBCA CP to clarify the purpose of archives records and to list the specific data required to be archived.

In December, 2009, the FPKIPA adopted a change to the FBCA CP that allows Certification Authorities (CAs) to implement remote administration without degrading FBCA CP operational and security requirements.

In January, 2010, the FPKIPA adopted a change to the FBCA CP to further align federal policy to emerging industry trends and lessons learned about reasonable compliance audit that ensure trust and assurances are being maintained.

The FPKI MA would like to maximize the operational efficiency of the FPKI by aligning the different CAs they manage by adopting the three operational changes to the FBCA CP in the EGCA CP.

Specific Changes: The specific changes for each of the three EGCA CP changes are listed below in separate sections.

Text with ~~strikethrough~~ will be removed. Underlined text will be added.

There are three specific changes for clarification of archiving:

1.) Remove last sentence of the first paragraph in section 4.5, *Security Audit Procedure*, which requires all audit records to be archived.

Audit log files shall be generated for all events relating to the security of the CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. ~~The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 4.5.3, *Retention Period for Security Audit Data*.~~

2.) Add text indicating that the requirements of NARA and/or other regulatory bodies must be followed. This text will be added to the beginning of section 4.6, *Records Archival*.

The EGCA's must follow either the General Records Schedules established by the National Archives and Records Administration or an agency-specific schedule as applicable.

3.) Modify the list in Section 4.6.1, *Types of Events Archived*, to add audit events that should be archived and clarify audit reporting requirements.

CA archive records will be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data will be recorded for archive:

- CA accreditation (if applicable)
- Certificate policy
- Certification practice statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of Re-key
- ~~Security audit data (in accordance with section 4.5)~~
- Revocation requests
- Subscriber identity authentication data as per section 3.1.9
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- Documentation of receipt of tokens

- All CRLs issued and/or published
- Other data or applications to verify archive contents
- ~~Documentation required by compliance auditors~~
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- The export of private and secret keys (keys used for a single session or message are excluded)
- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

~~In addition, CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys.~~

There are seven specific changes in support of remote administration.

2.1.7 Repository Obligations

All CAs that issue certificates under this policy are obligated to post all CA certificates and all CRLs in a directory that is publicly accessible through the Lightweight Directory Access Protocol. CAs may optionally post subscriber certificates in this directory in accordance with agency policy. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent modification or deletion of information.

4.5.4 Protection of Security Audit Data

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. CA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the ~~CA equipment~~ location where the data was generated.

5.1 PHYSICAL CONTROLS

CA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The CA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens shall be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to the EGCA, and any remote workstations used to administer the EGCA except where specifically noted.

5.1.1 Site Location and Construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

At a minimum, the physical access controls should—

- Ensure that no unauthorized access to the hardware is permitted
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two-person physical access control to both the cryptographic module and computer systems

Removable cryptographic modules shall be inactivated before storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and it shall not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs shall occur if the facility is to be left unattended.

6.5 COMPUTER SECURITY CONTROLS

Computer security controls are required to ensure CA/RA operations are performed as specified in this policy. The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to CA services and PKI roles

- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security-related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the CA system
- Enforce domain integrity boundaries for security-critical processes.

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements, the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure.

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

6.7 NETWORK SECURITY CONTROLS

A network guard, firewall, or filtering router must protect network access to CA equipment. The network guard, firewall, or filtering router shall limit services allowed to and from the CA equipment to those required to perform CA functions.

Protection of CA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CA equipment shall be necessary to the functioning of the CA application.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

There is one specific change for triennial audit.

2.7.1 Frequency of Entity Compliance Audit

CAs and RAs operating under this policy shall conduct a compliance audit no less than once every year. As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the Triennial Audit Guidance document located at <http://www.idmanagement.gov/fpkipa/>.

Additionally, the PA has the right to require aperiodic inspections of CAs and RAs to validate that the CA/RA is operating in accordance with their CPS.

Estimated Cost:

There is no financial cost associated with implementing this change.

Risk/Impact:

None. Positive impact is that operational requirements for the EGCA in the area of archive, audit and remote administration will be brought into alignment with the operational requirements of the Federal Bridge CA, making management of the FPKI CAs more efficient.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the EGCA Certificate Policy.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: August 5, 2010
Date presented to FPKIPA: August 10, 2010
Date of approval by FPKIPA: August 10, 2010