ARCHIVE REQUIREMENTS FOR
CERTIFIED PKI SHARED SERVICE PROVIDERS

January 29, 2007

The archive requirements are specified in the X.509 Certificate Policy for the Common Policy Framework (CCP) section 4.6, Records Archival. In this context, "archival" refers to management of records kept in long-term storage, physically separate from the CA or RA to which they pertain.[1] The general guidance for management of such records for Federal agency use is published in "Records Management Guidance For PKI-Unique Administrative Records", published at http://www.archives.gov/records_management/policy_and_guidance/pki_guidance.html , and at http://www.cio.gov/fpkisc/library/pki_rmg.pdf. Archival, in the present context, is addressed particularly in that document's section on Guidance for Recordkeeping Systems.

That guidance document pertains to administrative records, such as records about establishing, operating and terminating a CA. See chapter 4 of that document for a fuller discussion of this scope.

(Note: Similar guidance is being developed for PKI-unique transaction records, i.e., records of transactions that make use of PKI (such as digitally signed messages). Transaction records are within the purview of the agency, and therefore are outside the scope of the requirements of CCP section 4.6 that are elaborated here as applying to a service provider. However, if agencies want to outsource the function of archiving transaction records, that is a service that a service provider might want to offer as an option.)

"Records Management Guidance For PKI-Unique Administrative Records" distinguishes between PKI-unique records and PKI supporting records; see chapters 3, 4 and 5 of that document. PKI supporting records are those that pertain to most implementations of a computer or communications security infrastructure, and they are covered by records schedules or other guidance already existing when the guidance on PKI-unique records was being developed. Hence, both kinds of records for a PKI must be managed, and it may be convenient or efficient to manage them together. Both should be considered in the planning for compliance with the requirements of CCP section 4.6.

That guidance document distinguishes also between an Operational System (which maintains records in such a way that they can be accessed rapidly in the day-to-day activities of running a PKI, and potentially for a shorter time period than the authorized retention period) and a Recordkeeping System (which typically does not "create" records, but receives electronic records from an operational PKI system and other sources, and manages those records during their retention period). The requirements of CCP section 4.6 pertain to records that are transferred to and managed in a recordkeeping system, but since many of these records are

[1] In the terminology of the National Archives and Records Administration (NARA), "archival" refers to records whose retention period is unlimited, whereas time-limited records are called "temporary". In the PKI context, all records are likely to be temporary.

created in an operational system the planning for compliance with the requirements of CCP section 4.6 should consider the records created in the operational system (and other sources as explained in that guidance document) to assure that they will be available for archival.

That guidance document gives examples of ways to implement records capture, records metadata, records classification, records retrieval, records disposition, records integrity, records storage, records history log or audit trail, records privacy, records security, record freezes/holds, records transfer to a recordkeeping system, and long term records retention and preservation. These examples should be studied by the agency, and potential applicability of the sources cited there should be discussed between the Agency Records Officer and the NARA Appraisal Archivist. They should be studied also by the service provider, to anticipate agency requirements that the service provider will need to fulfill. For example, a freeze or hold could result in an extension of the retention period of the record(s) affected.

Note that each agency must submit an SF 115 to NARA for approval of a submitted records schedule. For the records management function, the legal requirements for Federal agencies depend on NARA policy and NARA approvals, as well as on the needs determined by agency management. The requirements of the CCP as elaborated here are requirements for service provider and agency participation in the Shared Service Provider program operating under the CCP.

In summary, compliance with the requirements of CCP section 4.6 will require planning for PKI supporting records as well as PKI-unique records, and planning for operational systems as well as recordkeeping systems. It will require planning for such further requirements as an agency may have for PKI administrative records (e.g., additional kinds of records, or a retention period for any or all PKI administrative records that exceeds the retention period required here, or a more frequent cutoff), as well as the "generic" set of requirements elaborated below. See, in particular, chapters 4 and 5, and appendix B, of "Records Management Guidance For PKI-Unique Administrative Records". It is the responsibility of each agency to ensure that they are retaining the appropriate PKI-unique administrative records and are employing all necessary records management guidance required to meet their regulatory, legal and business needs.

Subject to the qualification summarized in the foregoing paragraph as to what an agency may require of the service provider, the requirements of CCP section 4.6 as they apply generically to a service provider are here elaborated for CA and RA records, grouped as they relate to (a) the establishment and operation of the CA or RA as an entity; (b) its daily activities such as issuing certificates or preparing certificate requests from an RA to a CA; and (c) verifying the secure operation and trustworthiness of the CA and RA. Those required for CAs only or for RAs only are marked as "CA:" or "RA:"; all others pertain to CAs and RAs.

The archive retention period is 10 years and six months, following the date of the event ("cutoff") specified. This retention period follows the CCP, and agrees with the retention period for the Medium assurance level in the CP of the Federal Bridge.

The source records described below may be in any form (e.g., an applicant's Subscriber Agreement is likely to be in paper form, and most other records are likely to be electronic).[2]

The records are made routinely, and usually more frequently than they are archived. The cutoff determines the frequency of archiving.

A. RECORDS ESTABLISHING AND MAINTAINING THE CA OR RA AS AN ENTITY

CA: 1. Certificate Policy (CCP). Cutoff upon revision or reissuance, and at initiation or termination of the CA operation under that document.

CA: 2. Certification Practice Statement (CPS). Cutoff upon revision or reissuance, and at initiation or termination of the CA operation under that document.

3. Contractual Obligations and other agreements pertinent to operations under the CCP. Includes signed contracts, memoranda of agreement, memoranda of understanding, service level agreements. Includes agreements between a CA and its associated RAs or between an RA and its associated CAs and LRAs, and the applicable Certification Practice Statements (CPSs) and

[2]The Department of Defense is awaiting approval from NARA of a records disposition schedule that provides for the recordkeeping copy of subscriber agreements and related registration actions to be in electronic format. This means that those hard copy documents will be scanned into electronic format, and after the electronic copy has been verified the source documents will be destroyed. This is a step toward keeping all pki-unique administrative records in electronic form. Indeed, by use of such scanning and by use of digital signature where a signature is required, all documents covered by these Archive Requirements can be in electronic form for recordkeeping.

Following NARA approval of the Defense records schedule, a recommendation will be developed to incorporate a similar provision into these Archive Requirements, to require all CA and RA archive records to be kept in electronic form. SSPs and RAs should be prepared to employ digital signature where practical to avoid the reliance on hard copy source documents, and should be prepared, where source documents are in hard copy format, to convert them to electronic format for recordkeeping purposes.

Registration Authority Practice Statements (RPSs). Includes amended or revised versions of such documents, extensions thereto, applications for interoperability, evaluations of interoperability, and attestations of continued conformance with requirements. Cutoff upon expiration, termination, revision or reissuance of the document, and at initiation or termination of the CA or RA operation under such documents.

4. System and Equipment Configuration, Modifications, and Updates. This includes configuration change request, change form, and change logs. Cutoff upon revision or reissuance, and at initiation or termination of the CA or RA operation under the CCP or related documents.

5. Data or applications required for verifying archived contents. Cutoff upon revision or reissuance, and at initiation or termination of the CA or RA operation under the CCP or related documents.

6. Documentation of the records management plan. Cutoff upon revision or reissuance, and at initiation or termination of the CA or RA operation under the CCP or related documents.

B. RECORDS RELATING TO THE DAILY OPERATIONS OF THE CA OR RA

1. Copies of requests for issuance of the certificates and for their revocation/suspension/release. Cutoff quarterly.

CA: 2. Electronic copies of all certificates and CARLs/CRLs issued and/or published, and records of all certificate revocations, suspensions and releases. Cutoff quarterly.

RA: 3. Evidence that due diligence was exercised in validating the information contained in the certificate. For example, a copy of the documents used in authenticating the identity of the applicant for a certificate (e.g., a record of information supplied by or on behalf of the applicant, photocopy of identity credentials presented, photograph of applicant, template of fingerprint, reports from database queries). See CCP 3.1.8 and 3.1.9. Cutoff quarterly.

RA: 4. The signed original of each applicant's Subscriber Agreement (and Acknowledgment of Receipt of Token, if applicable). Cutoff quarterly.

CA: 5. Record of re-key. Cutoff upon re-key.

CA: 6. In addition, CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys. Cutoff quarterly.

B.1. BACKUPS

CA: 1. Behind-the-firewall directories. Cutoff quarterly.

CA: 2. Public directories. Cutoff quarterly.

CA: 3. Logs capturing information cycled into and out of directories. Cutoff quarterly.

4. System Backup. Cutoff quarterly.

C. RECORDS RELATING TO SECURITY AND TRUSTWORTHINESS OF THE CA OR RA

CA: 1. CA audit reports. Audit reports prepared by an independent auditor on CA's compliance with the CCP and the CA's CPS. Cutoff upon completion of subsequent clean audit report.

RA: 2. RA audit reports. Audit reports prepared by an independent auditor on RA's compliance with its RPS (or CPS). Cutoff upon completion of subsequent clean audit report.

CA: 3. Attestations of compliance by the CA's subordinate and cross-certified CAs, and of its associated RAs. Cutoff when subsequent attestation is received.
4. System Security Plans and Standard Operating Procedures. Documents detailing the measures in place to prevent compromise of physical plant, electronic intrusion, or CA employee malfeasance. Cutoff upon revision or reissuance.

5. CA and RA Certification and Accreditation, or similar documents as applicable. Cutoff upon revision or reissuance.

6. Documentation required by compliance auditors. Cutoff upon revision or reissuance.

C.1. SECURITY AUDIT LOGS.

The security audit logs include: a) the forms that are completed regularly on a daily, weekly, or monthly basis, b) the forms that are archived when these are completely filled and are replaced with new blank forms (e.g., Copy Control Forms), and c) forms that are completed as a result of occurrence of an events (e.g., Security Incidents Form). See CCP 4.5.

1. Records documenting system access by individuals, physical and electronic. Includes issuance of keys, passcards, accounts, and passwords. Cutoff quarterly.

2. Records resulting from the use of monitoring devices. This includes the videotapes, badge reader logs, and safe/secured container access logs. Cutoff quarterly.

3. Records resulting from daily and weekly system operational checks (e.g., daily and weekly system check lists). Cutoff quarterly.

4. Records resulting from the occurrence of events. This includes security incidents, help desk trouble-handling logs, and release of sensitive information. Cutoff quarterly.

5. Auditor's records. This includes auditor's checklist and audited items archival list. Cutoff quarterly.

-End-