| Criterion | |
|---|---|
| 4.5 | **CA Key Archival and Destruction** |
| | The CA maintains controls to provide reasonable assurance that:<br><br>• archived CA keys remain confidential and secured and are never put back into production;<br>• backup or additional copies of CA keys that no longer serve a valid business purposes are destroyed in accordance with the CA's disclosed business practices; and<br>• copies of CA keys are completely destroyed at the end of the key pair life cycle in accordance with the CA's disclosed business practices. |

| Illustrative Controls: | |
|---|---|
| | CA Key Archival |
| 4.5.1 | Archived CA keys are subject to the same or greater level of security controls as keys currently in use. |
| 4.5.2 | All archived CA keys are destroyed at the end of the archive period using dual control in a physically secure site. |
| 4.5.3 | Archived keys are only accessed where historical evidence requires validation. Control processes are required to ensure the integrity of the CA systems and the key sets. |
| 4.5.4 | Archived keys are recovered for the shortest possible time period technically permissible to meet business requirements. |
| 4.5.5 | Archived keys are periodically verified to ensure that they are properly destroyed at the end of the archive period. |
| | CA Key Destruction |
| 4.5.6 | The CA's private keys are not destroyed until the business purpose or application has ceased to have value or legal obligations have expired as disclosed within the CA's CPS. |
| 4.5.7 | Authorisation to destroy a CA private key and how the CA's private key is destroyed (e.g., token surrender, token destruction, or key overwrite) are limited in accordance with the CA's CPS. |
| 4.5.8 | All copies and fragments of the CA's private key are destroyed at the end of the key pair life cycle in a manner such that the private key cannot be retrieved. |
| 4.5.9 | If a secure cryptographic device is accessible and known to be permanently removed from service, all CA private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed. |

Deleted: completely

Deleted: and

Deleted:

Deleted: 0.1

| Illustrative Controls: | |
|---|---|
| 4.5.10 | If a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device. |
| 4.5.11 | If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed. |
| 4.5.12 | Backup or additional copies of CA keys that no longer serve a valid business purpose are destroyed in accordance with the CA's disclosed business practices. |
| 4.5.13 | The CA follows a CA key destruction script for key destruction ceremonies that includes the following:<br><br>a) definition and assignment of participant roles and responsibilities;<br>b) management approval for conduct of the key destruction ceremony;<br>c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be destroyed;<br>d) specific steps performed during the key destruction ceremony, including;<br>• HSM and/or cryptographic hardware zeroization/initialization<br>• HSM and/or cryptographic hardware physical destruction<br>e) physical security requirements for the ceremony location (e.g., barriers, access controls and logging controls);<br>f) procedures for secure storage of cryptographic hardware and any associated activation materials following the key destruction ceremony pending their disposal or additional destruction<br>g) sign-off on the script or in a log from participants and witnesses indicating whether the key destruction ceremony was performed in accordance with the detailed key destruction ceremony script; and<br>h) notation of any deviations from the key destruction ceremony script (e.g., documentation of steps taken to address any technical issues). |
| 4.5.14 | CA key destruction ceremonies are independently witnessed by internal or external auditors. |

**Formatted:** Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Indent at: 0.25"

**Deleted:** s

**Deleted:** s

**Formatted:** Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Indent at: 0.25"

**Deleted:** 0.1

| Criterion | |
|---|---|
| 4.9 | CA Key Transportation |
| | The CA maintains controls to provide reasonable assurance that:<br><br>• CA keys transported from one facility to another facility are prepared for transport in a physically secure environment (see §3.4), are stored in secure cryptographic modules in tamper-evident packaging, and require multi-person control by those in Trusted Roles to receive, access, and activate the CA keys;<br>• CA keys are transported separately from their corresponding activation materials;<br>• activation materials are transported in tamper-evident packaging;<br>• CA keys are transported in a method that prevents unauthorised access, activation, or use if intercepted or if otherwise not under multi-person control; and<br>• CA key transportation events are logged. |
| | ***Explanatory Guidance:*** CA Key Transportation refers to any event in which CA private signing keys are physically transported from one facility to another. This includes cases where the CA is migrating its production facility to another data centre, or when copies of the CA key are sent from the production facility to an alternate facility for backup or archive. It also includes situations in which the CA has acquired the CA keys from another entity, or has sold its CA keys to another entity.<br><br>Activation materials refers to passwords, PINs and/or tokens (i.e. m of n tokens) needed to access and/or activate the CA key on the secure cryptographic module and must not be transported together with the CA keys. |

| Illustrative Controls: | |
|---|---|
| 4.9.1 | CA keys are prepared for transport in a physically secure environment (see §3.4) by personnel in Trusted Roles and under multi-person control. |
| 4.9.2 | CA keys remain in a physically secure environment (see §3.4) until ready to be transported by CA personnel or common carrier. |
| 4.9.3 | CA keys are only transported on secure cryptographic devices and in tamper-evident packaging as disclosed in the CA's business practices. |
| 4.9.4 | If the secure cryptographic module contains the entire CA key, it is physically transported by at least two CA employees and remains under multi-person control from origin to destination. |

**Formatted:** List Paragraph, Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.25"

**Deleted:** 0.1

| Illustrative Controls: | |
|---|---|
| 4.9.5 | If the CA key is divided into fragments on multiple secure cryptographic modules:<br><br>a) If transported by CA employees, each fragment is transported separately using different transportation routes, methods, and/or times; or<br>b) If transported by common carrier, each fragment is sent using a different common carrier at different times. Shipments require signature service, tracking, and are insured. |
| 4.9.6 | Activation materials are transported separately from the CA key (i.e. by a different person or a different common carrier, and at different times) in tamper-evident packaging. |
| 4.9.7 | Upon receipt at the destination, packaging for CA keys and activation materials are reviewed for evidence of tampering. If evidence of tampering is discovered, the Policy Authority is notified of a possible breach event. |
| 4.9.8 | Upon receipt at the destination, CA keys and activation materials are stored in a physically secure environment (see §3.4) by personnel in Trusted Roles and under multi-person control. |
| 4.9.9 | Personnel involved in a CA key transportation events are in Trusted Roles and have received training in their role and responsibilities. |
| 4.9.10 | A log is maintained of all actions taken as part of the CA key transportation event and is retained in accordance with the CA's disclosed business practices. |
| 4.9.11 | Internal or external auditors accompany CA personnel during CA key transportation events. |

**Formatted:** List Paragraph, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Indent at: 0.25"

**Deleted:** 0.1

| Criterion | |
|---|---|
| 4.10 | CA Key Migration |
| | The CA maintains controls to provide reasonable assurance that:<br><br>• CA keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration (see §4.2), are completed in a physically secure environment (see §3.4) by those in Trusted Roles under multi-person control;<br>• hardware and software tools used during the CA key migration process are tested by the CA prior to the migration event; and<br>• CA key migration events are logged. |
| | ***Explanatory Guidance:*** CA Key Migration refers to events in which the CA is migrating its private signing keys from one secure cryptographic device to another. For example, this would encompass instances where the CA is upgrading from an older device model to a newer model, switching to a different hardware vendor, or migrating keys it acquired from another entity onto its own infrastructure. Routine backup and restorations (for example, transferring keys from a primary network hardware security module to a backup hardware security module token) when performed using approved methods from the hardware vendor are covered by Criterion 4.2. All other key movements between hardware devices are addressed by this Criterion 4.10. |

| Illustrative Controls: | |
|---|---|
| 4.10.1 | CA key migration events occur in a physically secure environment (see §3.4) by those in Trusted Roles under multi-person control. |
| 4.10.2 | Vendor-supplied hardware and software tools are tested by the CA prior the key migration event, and are operated in accordance with vendor-supplied documentation and instructions. |
| 4.10.3 | In-house developed software tools are developed and tested by the CA prior to the key migration event in accordance with its standard software development process (see §3.7). |

**Deleted:** 0.1

| Illustrative Controls: | |
|---|---|
| 4.10.4 | The CA follows a CA key migration script for key migration events that includes the following:<br><br>a) definition and assignment of participant roles and responsibilities;<br>b) management approval for conduct of the key migration event<br>c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be migrated and new hardware where the keys are being migrated to;<br>d) specific steps performed during the key destruction ceremony, including:<br>• Hardware preparation<br>• Software tool installation and setup<br>• Cryptographic hardware setup and initialisation<br>• CA key migration<br>• CA key verification<br>e) physical security requirements for the event location (e.g., barriers, access controls and logging controls);<br>f) procedures for secure storage of cryptographic hardware and any associated activation materials following the migration event<br>g) sign-off on the script or in a log from participants and witnesses indicating whether the key migration was performed in accordance with the detailed key migration script; and<br>h) notation of any deviations from the key migration script (e.g., documentation of steps taken to address any technical issues). |
| 4.10.5 | A log is maintained of all actions taken as part of the CA key migration event and is retained in accordance with the CA's disclosed business practices. |
| 4.10.6 | CA key migration events are witnessed by internal or external auditors. |
| 4.10.7 | Upon successful completion of a CA key migration event, remaining copies of the CA keys, and older cryptographic hardware that no longer serve a business purpose are securely destroyed in accordance with the CA's disclosed business practices (see §4.5). |

**Formatted:** Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Indent at: 0.25"

**Formatted:** Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Indent at: 0.25"

**Deleted:** 0.1

Deleted: 0.1