4.0: CA Key Lifecycle Management Controls

The Certification Authority maintains effective controls to provide reasonable assurance that the integrity of keys and certificates it manages is established and protected throughout their life cycles.

Criterion	
4.1	**CA Key Generation**
	The CA maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with the CA's disclosed business practices and defined procedures specified within detailed key generation ceremony scripts. The CA's disclosed business practices include but are not limited to: a) generation of CA keys are undertaken in a physically secured environment (see §3.4); b) generation of CA keys are performed by personnel in trusted roles (see §3.3) under the principles of multiple person control and split knowledge; c) generation of CA keys occur within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CPS; d) generation of CA keys are witnessed by an independent party and/or videotaped; and e) CA key generation activities are logged. The CA key generation script includes the following: a) definition of roles and participant responsibilities; b) approval for conduct of the key generation ceremony; c) cryptographic hardware and activation materials required for the ceremony; d) specific steps performed during the key generation ceremony; e) physical security requirements for the ceremony location; f) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony; g) sign-off from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and h) notation of any deviations from the key generation ceremony script.

Illustrative Controls:	
	Generation of CA Keys Including Root CA Keys – General Requirements
4.1.1	Generation of CA keys occur within a cryptographic module meeting the applicable requirements of ISO 15782-1/FIPS 140-2 (or equivalent)/ANSI X9.66 and the business requirements in accordance with the CPS. Such cryptographic devices perform key generation using a random number generator (RNG) or pseudo random number generator (PRNG).
4.1.2	The CA generates its own key pair in the same cryptographic device in which it will be used or the key pair is injected directly from the device where it was generated into the device where it will be used.

Illustrative Controls:	
4.1.3	CA key generation generates keys that: a) use a key generation algorithm as disclosed within the CA's CP and/or CPS; b) have a key length that is appropriate for the algorithm and for the validity period of the CA certificate as disclosed in the CA's CP and/or CPS. The public key length to be certified by a CA is less than or equal to that of the CA's private signing key; and c) take into account requirements on parent and subordinate CA key sizes and have a key size in accordance with the CA's CP and/or CPS.
4.1.4	CA key generation ceremonies are independently witnessed by internal or external auditors.
	Generation of CA Keys Including Root CA Keys – Script Requirements
4.1.5	The CA follows a CA key generation script for key generation ceremonies that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key generation ceremony; c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers; d) specific steps performed during the key generation ceremony, including; • Hardware preparation; • Verification of the integrity of the operating system and other software from its source (e.g. through the use of hash totals); • When a previously built master operating system image is being used, verification of the integrity of that image; • Operating system installation; • CA application installation and configuration; • CA key generation; • CA key backup; • CA certificate signing; • CA system shutdown; and • Preparation of materials for storage. e) physical security requirements for the ceremony location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony (e.g., detailing the allocation of materials between storage locations); g) sign-off on the script or in a log from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and h) notation of any deviations from the key generation ceremony script (e.g., documentation of steps taken to address any technical issues).
4.1.6	The integrity of the hardware/software used for key generation and the interfaces to the hardware/software is tested before production usage.

Deleted: which

Criterion	
4.2	**CA Key Storage, Backup, and Recovery**
	The CA maintains controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity. The CA's private keys are backed up, stored and recovered by authorised personnel in trusted roles, using multiple person control in a physically secured environment.

Illustrative Controls:	
4.2.1	The CA's private (signing and confidentiality) keys are stored and used within a secure cryptographic device meeting the appropriate ISO 15408 protection profile or FIPS 140-2 level requirement based on a risk assessment and the business requirements of the CA and in accordance with the CA's CPS and applicable Certificate Policy(s).
4.2.2	If the CA's private keys are not exported from a secure cryptographic module, then the CA private key is generated, stored and used within the same cryptographic module.
4.2.3	If the CA's private keys are exported from a secure cryptographic module to secure storage for purposes of offline processing or backup and recovery, then they are exported within a secure key management scheme that may include any of the following: a) as cipher-text using a key which is appropriately secured; b) as encrypted key fragments using multiple control and split knowledge/ownership; or c) in another secure cryptographic module such as a key transportation device using multiple control.
4.2.4	Backup copies of the CA's private keys are subject to the same or greater level of security controls as keys currently in use. The recovery of the CA's keys is carried out in as secure a manner as the backup process, using multi-person control.

Deleted:

Criterion	
4.3	CA Public Key Distribution
	The CA maintains controls to provide reasonable assurance that the integrity and authenticity of the CA public keys and any associated parameters are maintained during initial and subsequent distribution.

Illustrative Controls:	
4.3.1	For the Root CA distribution process (e.g., using a self-signed certificate), an out-of-band notification mechanism is employed. Where a self-signed certificate is used for any CA, the CA provides a mechanism to verify the authenticity of the self-signed certificate (e.g., publication of the certificate's fingerprint). For Intermediate, Issuing, and/or Subordinate CA public keys these are validated by using a chaining method or similar process to link back to the trusted Root Certificate.
4.3.2	The initial distribution mechanism for the CA's public key is controlled and initially distributed within a Certificate using one of the following methods: a) machine readable media (e.g., smart card, flash drive, CD ROM) from an authenticated source; b) embedding in an entity's cryptographic module; or c) other secure means that ensure authenticity and integrity.
4.3.3	The CA's public key is changed (rekeyed) periodically according to the requirements of the CPS with advance notice provided to avoid disruption of the CA services.
4.3.4	The subsequent distribution mechanism for the CA's public key is controlled in accordance with the CA's disclosed business practices.
4.3.5	If an entity already has an authenticated copy of the CA's public key, a new CA public key is distributed using one of the following methods: a) direct electronic transmission from the CA; b) placing into a remote cache or directory; c) loading into a cryptographic module; or d) any of the methods used for initial distribution.
4.3.6	The CA provides a mechanism for validating the authenticity and integrity of the CA's public keys.

Deleted: subsequent

Criterion	
4.4	CA Key Usage
	The CA maintains controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations.

Illustrative Controls:	
4.4.1	The activation of the CA private signing key is performed using multi-party control (i.e., m of n) with a minimum value of m (e.g., m greater than 2 for Root CAs).
4.4.2	If necessary based on a risk assessment, the activation of the CA private key is performed using multi-factor authentication (e.g., smart card and password, biometric and password, etc.).
4.4.3	CA signing key(s) used for generating certificates and/or issuing revocation status information, are not used for any other purpose.
4.4.4	The CA ceases to use a key pair at the end of the key pair's defined operational lifetime or when the compromise of the private key is known or suspected.
4.4.5	An annual review is required by the PA on key lengths to determine the appropriate key usage period with recommendations acted upon.

Criterion	
4.5	CA Key Archival
	The CA maintains controls to provide reasonable assurance that archived CA keys remain confidential, secured, and are never put back into production.

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.

Deleted: and Destruction

Deleted: :¶

Deleted: and

Deleted: ; and¶
CA keys are completely destroyed at the end of the key pair life cycle in accordance with the CA's disclosed business practices

Moved (insertion) [1]

Criterion	
4.6	CA Key Destruction
	The CA maintains controls to provide reasonable assurance that: • copies of CA keys that no longer serve a valid business purposes are destroyed in accordance with the CA's disclosed business practices; and • 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 Destruction
4.6.1	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.
4.6.2	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.
4.6.3	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.
4.6.4	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.
4.6.5	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.
4.6.6	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.
4.6.7	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.

Deleted: 5.

Deleted: 5.7

Deleted: 5.8

Deleted: 5.9

Deleted: .10

Deleted: 5.11

Illustrative Controls:	
4.6.8	The CA follows a CA key destruction script for key destruction ceremonies that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key destruction ceremony; c) specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be destroyed; d) specific steps performed during the key destruction ceremony, including; a. HSM and/or cryptographic hardware zeroisation/initialisation b. HSM and/or cryptographic hardware physical destruction c. Deletion of any encrypted files containing the CA key or fragments thereof e) physical security requirements for the ceremony location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and any associated activation materials following the key destruction ceremony pending their disposal or additional destruction 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 h) notation of any deviations from the key destruction ceremony script (e.g., documentation of steps taken to address any technical issues).
4.6.9	CA key destruction ceremonies are independently witnessed by internal or external auditors.

Moved (insertion) [2]

Criterion	
4.7	CA Key Compromise
	The CA maintains controls to provide reasonable assurance that continuity of operations is maintained in the event of the compromise of the CA's private keys and any certificates, signed with the compromised keys, are revoked and reissued.

Illustrative Controls:	
4.7.1	The CA's business continuity plans address the compromise or suspected compromise of a CA's private keys as a disaster.
4.7.2	Disaster recovery procedures include the revocation and reissuance of all certificates that were signed with that CA's private key, in the event of the compromise or suspected compromise of a CA's private signing key.
4.7.3	The recovery procedures used if the CA's private key is compromised include the following actions: a) how secure key usage in the environment is re-established; b) how the CA's old public key is revoked; c) how affected parties are notified (e.g., impacted CAs, Repositories, Subscribers and CVSPs); d) how the CA's new public key is provided to the end entities and Relying Parties together with the mechanism for their authentication; and e) how the subscriber's public keys are re-certified.
4.7.4	In the event that the CA has to replace its Root CA private key, procedures are in place for the secure and authenticated revocation of the following: a) the old CA root public key; b) the set of all certificates (including any self-signed) issued by a Root CA or any CA based on the compromised private key; and c) any subordinate CA public keys and corresponding certificates that require recertification.
4.7.5	The CA's business continuity plan for key compromise addresses who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures and encrypted data.

Moved up [1]: ¶
Page Break
¶
Criterion

Deleted: 4.6 ...

Deleted: 6

Deleted: 6

Deleted: 6

Deleted: 6

Deleted: 6

Moved (insertion) [3]

Criterion	
4.8	CA Cryptographic Hardware Life Cycle Management
	The CA maintains controls to provide reasonable assurance that: • devices used for private key storage and recovery, and the interfaces to these devices are tested before usage for integrity; • access to CA cryptographic hardware is limited to authorised personnel in trusted roles, using multiple person control; and • CA cryptographic hardware is functioning correctly.

Illustrative Controls:	
4.8.1	CA cryptographic hardware which does not contain CA keys is sent from the manufacturer or alternate CA site via registered mail (or equivalent) using tamper evident packaging. Upon the receipt of CA cryptographic hardware from the manufacturer or alternate site, authorised CA personnel inspects the tamper evident packaging to determine whether the seal is intact.
4.8.2	Upon the receipt of CA cryptographic hardware from the manufacturer, acceptance testing and verification of firmware settings is performed. Upon the receipt of CA cryptographic hardware that has been serviced or repaired, acceptance testing and verification of firmware settings is performed.
4.8.3	To prevent tampering, CA cryptographic hardware is stored and used in a secure site, with access limited to authorised personnel, having the following characteristics: a) inventory control processes and procedures to manage the origination, arrival, condition, departure and destination of each device; b) access control processes and procedures to limit physical access to authorised personnel; c) recording of all successful or failed access attempts to the CA facility and device storage mechanism (e.g., a safe) in audit logs; d) incident handling processes and procedures to handle abnormal events, security breaches, and investigation and reports; and e) monitoring processes and procedures to verify the ongoing effectiveness of the controls.
4.8.4	When not attached to the CA system, the CA cryptographic hardware is stored in a tamper resistant container that is stored securely under multiple controls (i.e., a safe).

Moved up [2]: ¶
Page Break
¶
Criterion

Deleted: 4.7 ...

Deleted: 7

Deleted: 7

Deleted: 7

Deleted: 7

Illustrative Controls:	
4.8.5	The handling of CA cryptographic hardware, including the following tasks, is performed in the presence of no less than two trusted employees: a) installation of CA cryptographic hardware; b) removal of CA cryptographic hardware from production; c) servicing or repair of CA cryptographic hardware (including installation of new hardware, firmware, or software); and d) disassembly and permanent removal from use.
4.8.6	Devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity.
4.8.7	Correct processing of CA cryptographic hardware is verified on a periodic basis.
4.8.8	Diagnostic support is provided during troubleshooting of CA cryptographic hardware in the presence of no less than two trusted employees.

Deleted: 7

Deleted: 7

Deleted: .7

Deleted: 7

Criterion	
4.9	CA Key Escrow (if applicable)
	The CA maintains controls to provide reasonable assurance that escrowed CA private signing keys remain confidential.
	Explanatory Guidance: CA Key Escrow refers to the practice of a third-party holding a copy (e.g. backup copy, archive copy etc.) of the CA's private signing key on its behalf. If the CA has not escrowed any of its CA keys to a third-party, then Criterion 4.8 is not applicable.

Illustrative Controls:	
4.9.1	If a third party provides CA private key escrow services, a contract exists that outlines the liabilities and remedies between the parties.
4.9.2	If CA private signing keys are held in escrow, escrowed copies of the CA private signing keys have the same or greater level of security controls as keys currently in use.

Moved up [3]: ¶
Page Break
¶
Criterion

Deleted: 4.8 ...

Deleted: 8

Deleted: 8

Criterion	
4.10	CA Key Transportation (if applicable)
	The CA maintains controls to provide reasonable assurance that: • CA private keys that are physically transported from one facility to another remain confidential and maintain their integrity; • CA hardware containing CA private keys, and associated activation materials, are prepared for transport in a physically secure environment (see §3.4) by authorised personnel in trusted roles, using multiple person controls, and are transported within sealed tamper evident packaging; • CA keys and associated activation materials are transported in a manner that prevents the key from being activated or accessed during the transportation event; and • 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. Activation materials refers to items including but not limited to passwords, PINs, tokens (i.e. m of n tokens) and/or key-wrapping keys needed to access and/or activate the CA key on the secure cryptographic module and must not be transported together with the CA keys. The intent of this criterion is for CA keys to maintain their confidentiality and integrity during transportation, and to be transported in a manner that prevents the keys from being activated or accessed during their transportation, including transporting associated activation materials separately. The methods to accomplish this vary based on the circumstances of how the CA keys are stored and protected. For example, some cryptographic hardware store keys directly within the device, whereas others store the key in an encrypted form on a client file system (i.e. on a hard disk) with the master key stored on a series of activation cards and utilise the cryptographic device to access the content of the client file system. Different considerations for transportation and security will need to be applied in both of those examples.

Illustrative Controls:	
4.10.1	CA keys are prepared for transport in a physically secure environment (see §3.4) by personnel in Trusted Roles and under multi-person control.
4.10.2	CA keys remain in a physically secure environment (see §3.4) until ready to be transported by CA personnel or common carrier.
4.10.3	CA keys are only transported on hardware devices and in tamper-evident packaging as disclosed in the CA's business practices.

Illustrative Controls:	
4.10.4	If the hardware device 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.
4.10.5	If the CA key is divided into fragments on multiple hardware devices: a) If transported by CA employees, each fragment is transported separately using different transportation routes, methods, and/or times; or b) If transported by common carrier, each fragment is sent using a different common carrier at different times. Shipments require signature service, tracking, are insured.
4.10.6	Activation materials are transported separately from the CA key (i.e. by a different method and/or at a different time) in tamper-evident packaging.
4.10.7	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.
4.10.8	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.
4.10.9	Personnel involved in a CA key transportation event are in Trusted Roles and have received training in their role and responsibilities.
4.10.10	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.
4.10.11	Internal or external auditors accompany CA personnel during CA key transportation events.

Criterion	
4.11	CA Key Migration (if applicable)
	The CA maintains controls to provide reasonable assurance that: • 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; • hardware and software tools used during the CA key migration process are tested by the CA prior to the migration event; and • CA key migration events follow a documented script and 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:	
4.11.1	CA key migration events occur in a physically secure environment (see §3.4) by those in Trusted Roles under multi-person control.
4.11.2	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.
4.11.3	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).

Illustrative Controls:	
4.11.4	The CA follows a CA key migration script for key migration events that includes the following: a) definition and assignment of participant roles and responsibilities; b) management approval for conduct of the key migration event 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; d) specific steps performed during the key migration ceremony, including: • Hardware preparation • Software tool installation and setup • Cryptographic hardware setup and initialisation • CA key migration • CA key verification e) physical security requirements for the event location (e.g., barriers, access controls and logging controls); f) procedures for secure storage of cryptographic hardware and any associated activation materials following the migration event 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 h) notation of any deviations from the key migration script (e.g., documentation of steps taken to address any technical issues).
4.11.5	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.
4.11.6	CA key migration events are witnessed by internal or external auditors.
4.11.7	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).