Criteria	Control ID	Control source	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor
1 - CA Key Generation	1.1	WebTrust 4.1.1	Generation of CA keys occur within a cryptographic module meeting the applicable requirements of ISO 19790 and ISO 13491-1/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).	Inspection of key management policy and procedures to confirm generation of keys happens in a cryptographic module meeting the requirements. Selection of a sample of CA certificates with the OCSP signing EKU included to confirm generation of keys happened within a cryptographic module meeting the requirements.
	1.2	WebTrust 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.	Inspection of key management policy and procedures to confirm CA keys are injected directly from the device where it was generated into the device where it will be used. Selection of a sample of CA certificates with the OCSP signing EKU included to confirm the keys have been injected directly from the device where they were generated into the device where they were used.
	1.3	WebTrust 4.1.4	CA key generation ceremonies are independently witnessed by internal or external auditors.	Inspection of key management policy and procedures to confirm CA key generation ceremonies require to be independently witnessed by internal or external auditors. Selection of a sample of CA certificates with the OCSP signing EKU included to confirm the CA key generation ceremonies were independently witnessed by internal or external auditors.
	1.4	WebTrust 4.1.5	Generation of CA keys shall be undertaken in a physically secured environment (see §3.4) by personnel in trusted roles (see §3.3) under the principles of multiple control and split knowledge.	Inspection of the key management policy and procedures to confirm CA key generation ceremonies are undertaken in a physically secured environment by personnel in trusted roles using the principle of multiple control and split knowledge. Selection of a sample of CA certificates with the OCSP signing EKU included in order to verify these key generation ceremonies have been undertaken in a physically secured environment by personnel in trusted roles using the principle of multiple control and split knowledge.

Criteria	Control ID	Control source	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor
	1.5	WebTrust 4.1.6	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).	Inspection of the key management policy to confirm key generation scripts do include the items described in the control. Selection of a sample of CA certificates with the OCSP signing EKU included to verify the key generation scrips / logs of these key ceremonies include the items described in the control.
2 - CA Key Storage, Backup, and Recovery	2.1	WebTrust 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).	Inspection of the key management policy and procedures to confirm CA private keys are stored and used within a secure cryptographic device, based on risk assessment and in accordance with the CP and CPS. Selection of a sample of CA certificates with the OCSP signing EKU set to ensure they are stored and used within a secure cryptographic device.
	2.2	WebTrust 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.	Inspection of the key management policy and procedures and system design to confirm CA private keys are not exported from a secure cryptographic module.

Criteria	Control ID	Control source	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor
	2.3	WebTrust 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.	Inspection of the key management policy and procedures to confirm that CA private keys are exported as encrypted key fragments using multiple control and split knowledge/ownership when they are exported from a secure cryptographic module to secure storage for purposes of offline processing or backup and recovery. Selection of a sample of CA certificates with the OCSP signing EKU included in order to confirm they were exported to secure storage for purposes of offline processing or backup and recovery as encrypted key fragments using multiple control and split knowledge/ownership.
	2.4	WebTrust 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.	Inspection of all CA private key backup facilities to confirm they are subject to the same or greater level of security controls as keys currently in use. Inspection of a sample of key recovery logs to confirm that the recovery is carried out in as secure a manner as the backup process, using multi-person control.
	2.5	GlobalSign internal	Active issuing CA private keys are located in a physically segregated zone (room) with multi-person access controls. This physical zone only contains systems capable of issuing certificates.	Inspection of all CA facilities to confirm CA private keys are located in a physically segregated zone with multi-person access control. Inspection of all CA facilities to confirm the physical zone in which CA private keys are located does only contain systems capable of issuing certificates.
3 - CA Key Usage	3.1	WebTrust 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).	Inspection of the key management policy and procedures and system design to confirm the activation of the CA private signing key requires multi-party control.
	3.2	WebTrust 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.).	Inspection of the key management policy and procedures and system design to confirm the activation of CA private keys requires multi-factor authentication.
	3.3	GlobalSign internal	CA signing key(s) used for generating certificates and/or issuing revocation status information through Certificate Revocation Lists (CRL), are not used for any other purpose, including OCSP response signing.	Inspection of the system design to confirm CA signing keys are only used for generating certificates and issuing revocation status information through Certificate Revocation Lists. Selection of a sample of CA certificates with the OCSP signing EKU included in order to confirm they have only been used for generating certificates and issuing revocation status information through Certificate Revocation Lists.
4 - CA Key Destruction	4.1	WebTrust 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.	Inspection of the key management policy and procedures to confirm key destruction practices ensure 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. For all destroyed CA certificates with the OCSP signing EKU included, confirmation that all copies and fragments of these CA private keys have been destroyed in a manner such that the private key cannot be retrieved.

Criteria	Control ID	Control source	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor
	4.2	WebTrust 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).	Inspection of the key management policy and procedures to confirm key destruction practices and scripts include the items described in the control. For all destroyed CA certificates with the OCSP signing EKU included, confirmation that the key generation scrips / logs of these key ceremonies include the items described in the control.
	4.3	WebTrust 4.6.9	CA key destruction ceremonies are independently witnessed by internal or external auditors.	Inspection of key management policy and procedures to confirm CA key destruction ceremonies require to be independently witnessed by internal or external auditors. For all destroyed CA certificates with the OCSP signing EKU included, confirm the destruction ceremony was independently witnessed by internal or external auditors.
5 - OCSP Signing	5.1	GlobalSign internal	Only OCSP responder leaf certificates are used for signing OCSP responses on behalf of issuing CA.	Inspection of a sample of OCSP responders to confirm that OCSP responders are configured with OCSP responder leaf certificates.
	5.2	Baseline Requirements 4.9.9	OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST either: 1.Be signed by the CA that issued the Certificates whose revocation status is being checked, or 2.Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.	Inspection of a sample of OCSP responders' configuration and OCSP responses to confirm they are: - RFC 6960 and/or RFC5019 compliant - Signed by an OCSP responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked - The OCSP responder Certificates contain an extension of type id-pkix-ocsp-nocheck as defined by RFC6960.
	5.3	GlobalSign internal	OCSP signing is performed using systems dedicated to this purpose, only these systems have OCSP signing keys loaded.	Inspection of the system design and architecture to confirm OCSP responses are signed from systems dedicated for this purpose. Inspection of key management policy and procedures to confirm OCSP signing certificates are generated within the cryptographic devices supporting the OCSP signing systems.

Criteria	Control ID	Control source	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor
6 - Logical Security	6.1	GlobalSign internal	Network communication in the CA issuance systems network segment is limited to outbound push/pull queue traffic. No other interactions between the CA issuance segment and other networks are possible.	Inspection of the system design and architecture to confirm communication with CA issuance systems is designed so that it is limited to outbound push/pull queue traffic and no other network interactions between the CA issuance segment and other networks are possible.
	6.2	GlobalSign internal	CA issuance systems are stripped of any unnecessary functionality and do not contain the necessary software to automatically generate and/or sign OCSP responses.	Inspection of a sample of CA issuance systems to confirm they do not contain the necessary software to automatically generate and/or sign OCSP responses.
	6.3	WebTrust 3.7.3	Change control procedures exist and are followed for the hardware, network component, and system configuration changes.	Inspection of change control procedures for hardware, network component and system configuration changes. Inspection of a sample of hardware, network component and system configuration changes to confirm that change control procedures were followed.
	6.4	GlobalSign internal	Changes to network and security components supporting CA issuance systems require approval from the security team and changes are monitored independently by the Security Operations Center (SOC)	Inspection of a sample of changes to network and security components supporting CA issuance systems to confirm that approval was provided, and monitoring was performed.
	6.4	GlobalSign internal	Network traffic to CA issuance systems is limited to outbound push/pull queuing, using a structured protocol for certificate issuance and revocation. The mechanism does not support the exchange of OCSP related messages.	Inspection of a sample of firewall rules on the network zone for CA issuance systems to confirm only outbound push/pull traffic is allowed. Inspection of the protocol for certificate issuance and revocation to confirm OCSP related messaging is not supported.
7 - Audit logging	7.1	GlobalSign internal	CA key signing actions on CA issuance systems are logged.	Inspection of the audit logging policy to confirm it requires each CA key signing action to be logged. Inspection of a sample of key signing actions to confirm that actions are logged.
	7.2	GlobalSign internal	CA signing logs are retained for at least 10 years.	Inspection of the CP and CPS and audit logging policy to confirm it requires signing logs to be retained for at least 10 years. Inspection of a sample of CA signing logs to confirm retention period.
	7.3	GlobalSign internal	Configuration records and system change logs are maintained for all systems involved in CA operations.	Inspection of the change control and audit logging policy to confirm it requires configuration records and system change logs to be maintained for all systems involved in CA operations. Inspection of a sample of systems involved in CA operations related to issuance and signing to confirm configuration records and system change logs are maintained.
	7.4	WebTrust 3.10.1	The CA generates automatic (electronic) and manual audit logs in accordance with the requirements of the CP and/or CPS.	Inspection of a sample of audit logs of systems involved in CA operations to confirm the logs are generated in accordance with the requirements of the CP and/or CPS.
	7.5	WebTrust 3.10.2	All journal entries include the following elements: a) date and time of the entry; b) serial or sequence number of entry (for automatic journal entries); c) kind of entry; d) source of entry (e.g., terminal, port, location, customer, etc.); and e) identity of the entity making the journal entry.	Inspection of the audit logging policy to confirm it requires journal entries to contain the information described in the control. Inspection of a sample of logs from systems involved in CA operations related to issuance and signing to confirm the journal entries contain the information described in the control.

Criteria	Control ID	Control source	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor
	7.6	WebTrust 3.10.3	The CA logs the following CA and subscriber (if applicable) key life cycle management related events: a) CA key generation; b) installation of manual cryptographic keys and its outcome (with the identity of the operator); c) CA key backup; d) CA key storage; e) CA key recovery; f) CA key escrow activities (if applicable); g) CA key usage; h) CA key archival; i) withdrawal of keying material from service; j) CA key destruction; k) CA key transportation; l) CA key migration m) identity of the entity authorising a key management operation; n) identity of the entities handling any keying material (such as key components or keys stored in portable devices or media); o) custody of keys and of devices or media holding keys; and p) compromise of a private key.	Inspection of the key management policy and procedures to confirm it requires the logging of the key life cycle management related events described in the control. Selection of a sample of CA certificates with the OCSP signing EKU included in order to confirm the key life cycle management related events described in the control have been logged.