WebTrust requirement not covered in CCA checklist

	WebTrust	Type
3.3	Personal Security	
3.3.12	If required based on a risk assessment, duress alarms are provided for users who might be the target of coercion.	Installation
3.4	Physical and Environmental Security	
3.4.2	All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organisation's other systems so that only authorised employees of the CA can access them.	Data Centre selection, additional security
	Network access control	
3.6.12	Access to diagnostic ports is securely controlled.	Process update and document
3.6.20	Automatic terminal identification is used to authenticate connections to specific locations and to portable equipment.	Process update and document
	Key Generation Script	
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.	Process update and document

	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).	
	CA-provided subscriber key archival	
5.2.6	Subscriber private (confidentiality) keys archived by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the requirements of the CP.	Process update and document
5.2.7	If the CA provides subscriber (confidentiality) key archival, all archived Subscriber keys are destroyed at the end of the archive period	
	CA-provided subscriber key destruction	
5.2.8	If the CA provides subscriber (confidentiality) key storage, authorisation to destroy a subscriber's private key and the means to destroy the subscriber’s private (confidentiality) key (e.g., key overwrite) is limited in accordance with the CP.	Process update and document
5.2.9	If the CA provides subscriber (confidentiality) key storage, all copies and fragments of the subscriber's private key are destroyed at the end of the key pair life cycle.	
	CA-provided subscriber key escrow	
5.2.10	Subscriber private (confidentiality) keys escrowed by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the requirements of the CP	Process update and document
5.3	Integrated Circuit Card (ICC) Lifecycle Management (if supported	
	ICC procurement	New service
5.3.1	If the CA or RA engages a card bureau then a formal contract exists between the relevant parties. While card issuing functions may be delegated to third parties the CA retains responsibility and liability for the ICCs	SW upgrade to card issuance Process update and document
5.3.2	ICCs are logically protected during transport between the card manufacturer and the card issuer through the use of a secret transport key or pass phrase	Process update and document
5.3.3	ICCs issued to subscribers meet the appropriate ISO 15408 protection profile, ISO card standard (e.g., ISO 7810, 7811 parts 1-5, 7813, 7816, 10202) or FIPS 140-2 level requirement based on a risk assessment and the requirements of the CP.	
5.3.4	The card bureau verifies the physical integrity of ICCs upon receipt from the card manufacturer	
5.3.5	ICCs are securely stored and under inventory control while under the control of the card issuer	
	Card preparation and personalisation	
5.3.6	The CA (or RA), as the card issuer, controls ICC personalisation (the loading of Common Data File (CDF) data and its related cryptographic keys).	Process update and document

5.3.7	Common data that identify the ICC, the card issuer, and the cardholder are stored by the card issuer in the ICC Common Data File (CDF). Common Data File (CDF) activation is performed by the CA (or RA), as the card issuer, using a securely controlled process.	
5.3.8	ICC preparation processes and procedures, including the following, exist and are followed: a. loading of the card operating system; b. creation of logical data structures (card file system and card security domains); c. loading of applications; and d. logically protecting the ICC to prevent unauthorised modification of the card operating system, card file system, card security domains, and applications.	
5.3.9	ICC personalisation processes and procedures, including the following, exist and are followed: a. the loading of identifying information onto the card; b. generation of subscriber key pair(s) in accordance with the CP; c. loading subscriber private key(s) onto the ICC (if generated outside the card) in encrypted form; d. loading subscriber Certificate(s) onto the ICC; e. loading the CA and other Certificates for the contractual environment onto the ICC; and f. logically protecting the ICC from unauthorised access.	
5.3.10	The card bureau or CA (or RA) logs ICC preparation and personalisation in an audit log.	
5.3.11	An ICC is not issued unless the card has been prepared and personalised by the card bureau, the CA or the RA	
5.3.12	An ICC is unusable unless in an activated or reactivated state	
	ICC storage and distribution	
5.3.13	ICCs are securely stored prior to distribution.	Storage
5.3.14	Processes and procedures exist and are followed for the distribution, tracking and accounting for the safe receipt of Subscriber ICCs to subscribers.	Process update and document
5.3.15	ICC initial activation data (initialising PIN) is securely communicated to the subscriber or where applicable the Subscriber using an out-of-band method. The subscriber is encouraged to change the initial activation data upon receipt to make the card active	
5.3.16	ICC distribution is logged by the card bureau or CA (or RA) in an audit log.	
	Subscriber ICC usage	
5.3.17	The subscriber is provided with a mechanism that protects the access to the card data including the private keys stored on the ICC during use by the Subscriber (i.e., PIN access control mechanism Cardholder Verification Method)	Process update and document
5.3.18	The subscriber private keys on the ICC are not exported to an application to undertake cryptographic (i.e., signing) functions.	
5.3.19	The subscriber is required to use a mutual authentication mechanism for cryptographic application and card functions to ensure system integrity	SW upgrade Process update and document
5.3.20	The subscriber is required to use an application that displays the message or the message's digest to the subscriber prior to signing message (or transaction) data. The subscriber ICC application produces audit logs of all uses of the ICC. This also includes all attempts in the private key owner verification process.	Process update and document

5.3.21	The ICC is used by the subscriber or where applicable the Subscriber in accordance within the terms of the CP.	
	ICC deactivation and reactivation	
5.3.22	Application Data File (ADF) deactivation can be performed only by the CA, as the application supplier.	Process update and document
5.3.23	Common Data File (CDF) deactivation can be performed only by the CA, as the card issuer.	
5.3.24	CDF reactivation is conducted under the control of the CA, as the card issuer.	
5.3.25	ADF reactivation is conducted under the control of the CA, as the application supplier	
5.3.26	ADF deactivation, CDF deactivation, CDF reactivation, and ADF reactivation are logged.	
	ICC replacement	
5.3.27	Processes and procedures exist and are followed for replacement of a subscriber's lost or damaged ICC.	Process update and document
5.3.28	In the event of card loss or damage, subscriber certificates are renewed or rekeyed in accordance with the CP (see clauses 6.2 and 6.3).	
5.3.29	ICC replacement is logged by the card bureau or CA (or RA) in an audit log.	
	ICC termination	
5.3.30	All ICCs returned to the ICC or CA (or RA) are deactivated or securely destroyed to prevent unauthorised use.	Process update and document
5.3.31	Common Data File (CDF) termination is controlled by the CA, as the card issuer.	
5.3.32	ICC termination is logged by the card bureau or CA (or RA) in an audit log.	
6.6	Life cycle technical controls	
6.6.1	System development controls	Process update and document
6.6.2	Security management controls	
6.6.3	Life cycle security controls	
6.3	Certificate Rekey	
6.3.3	For authenticated certificates, the CA or the RA processes the Certificate Rekey Request to verify the identity of the requesting entity and identify the certificate to be rekeyed	Process update and document
6.3.4	For domain validated certificates, the CA or the RA process the Certificate Rekey Request to re-validate the domain in accordance with the requirements of the CP.	
6.3.5	The CA or the RA validates the signature on the Certificate Rekey Request	
6.3.6	The CA or the RA verifies the existence and validity of the certificate to be rekeyed.	
6.3.7	The CA or the RA verifies that the Certificate Rekey Request meets the requirements defined in the relevant CP.	
6.3.8	If an external RA is used, the CA requires that RAs submit the entity's certificate rekey request to the CA in a message signed by the RA	
6.3.9	If an external RA is used, the CA requires that the RA secure that part of the certificate rekey process for which it (the RA) assumes responsibility.	

6.3.10	If an external RA is used, the CA requires that external RAs record their actions in an audit log	
6.3.11	If an external RA is used, the CA verifies the RA's signature on the Certificate Rekey Request.	
6.3.12	The CA or the RA checks the Certificate Rekey Request for errors or omissions.	
6.3.13	The CA or RA notifies Subscribers prior to the expiration of their certificate of the need for rekey	
6.3.14	Prior to the generation and issuance of rekeyed certificates, the CA or RA verifies the following: a. the signature on the certificate rekey data submission; b. the existence and validity supporting the rekey request; and c. that the request meets the requirements defined in the CP.	
7	Subordinate CA and Cross Certificate Lifecycle Management Controls	
7.1	Subordinate CA Certificate and Cross Certificate Lifecycle Management	
	Subordinate CA (Sub-CA) and cross certificate registration	
7.1.1	The Parent CP specifies the requirements for submission of Sub-CA and cross certification requests.	Additional HSM
7.1.2	The Parent CA authenticates the Sub-CA or cross certificate request in accordance with the Parent's CP.	Process update and document
7.1.3	The Parent CA performs an assessment of the Sub-CA or cross certificate applicant's compliance with the requirements of the Parent CA's CP before approving a Sub-CA or cross certificate request, or alternatively the Sub-CA or cross certificate applicant presents its CPS for assessment	
	Sub-CA and cross certificate renewal	
7.1.4	Where Sub-CA and cross certificate renewal is permitted, the Parent CA's CP specifies the requirements for submission of Sub-CA or cross certificate renewal requests	Process update and document
7.1.5	Where Sub-CA certificate and cross certificate renewal is permitted, the Parent CA authenticates the Sub-CA or cross certificate renewal request in accordance with the CA's CP.	
	Sub-CA and cross certificate rekey	
7.1.6	The Parent CA's CP specifies the requirements for submission of Sub-CA rekey requests.	Process update and document
7.1.7	The Parent CA authenticates the Sub-CA certificate rekey request in accordance with the CP	
	Sub-CA and cross certificate issuance	
7.1.8	The Parent CA generates certificates: a. using the appropriate certificate profile in accordance with the CP and ISO 9594/X.509 and ISO 15782-1 formatting rules; b. with the validity periods formatted in accordance with ISO 9594/X.509, ISO 15782-1 and the CP; and c. where extensions are used, with extension fields formatted in accordance with ISO 9594/X.509, ISO 15782-1 and the CP.	Process update and document
7.1.9	The Parent CA signs the Sub-CA or cross certificate with the Parent CA's private signing key	
	Sub-CA and cross certificate distribution	
7.1.10	The Parent CA makes Sub-CA and cross certificates available to relevant entities (e.g., Relying Parties) using an established mechanism (e.g., a repository such as a directory) in accordance with the Parent CA's CP	Process update and document

	Sub-CA and cross certificate revocation	
7.1.11	The Parent CA verifies the identity and authority of the entity requesting revocation of a Sub-CA or cross certificate in accordance with the Parent CA's CP.	Process update and document
7.1.12	The Parent CA updates the Certificate Revocation List (CRL) and other Sub-CA or cross certificate status mechanisms upon certificate revocation in accordance with the Parent CA's CP.	
	Sub-CA and cross certificate status information processing	
7.1.13	The Parent CA makes Sub-CA and cross certificate status information available to Relying Parties using an established mechanism (e.g., CRL, OCSP, etc.) in accordance with the Parent CA's CP.	Process update and document

Browser Forum requirement not covered in CCA checklist

Controls	Requirement	Type
2.3	• The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. • The CA SHALL indicate conformance with this requirement by incrementing the version number and adding a dated change log entry, even if no other changes are made to the document.	Process update and document
3.1.6	Recognition, authentication, and role of trademarks	
3.2.2.1	The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following: 1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition; 2. A third party database that is periodically updated and considered a Reliable Data Source; 3. A site visit by the CA or a third party who is acting as an agent for the CA; or 4. An Attestation Letter.	
3.2.2.2	DBA/Tradename If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following: 1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition; 2. A Reliable Data Source; 3. Communication with a government agency responsible for the management of such DBAs or trade names;	

	4. An Attestation Letter accompanied by documentary support; or 5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.	
3.2.2.3	Verification of Country If the subject: country Name field is present, then the CA SHALL verify the country associated with the Subject using one of the following: a. the IP Address range assignment by country for either I. the web site's IP address, as indicated by the DNS record for the web site or a. the Applicant's IP address; b. the ccTLD of the requested Domain Name; c. information provided by the Domain Name Registrar; or d. a method identified in Section 3.2.2.1.	Process update and document, Tool may be used
3.2.2.4	Validation of Domain Authorization or Control This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain. The CA SHALL confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate as follows: 1. When the FQDN is not an Onion Domain Name, the CA SHALL validate the FQDN using at least one of the methods listed below; and 2. When the FQDN is an Onion Domain Name, the CA SHALL validate the FQDN	
3.2.2.4	CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.	
3.2.2.4.1	Validating the Applicant as a Domain Contact This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.	NA
3.2.2.4.2	Email, Fax, SMS, or Postal Mail to Domain Contact Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.	Process update and document

3.2.2..4.3	Phone Contact with Domain Contact This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.	NA
3.2.2.4.4	Constructed Email to Domain Contact Confirm the Applicant’s control over the FQDN by 1. Sending an email to one or more addresses created by using ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’, or ‘postmaster’ as the local part, followed by the at-sign (“@”), followed by an Authorization Domain Name; and 2. including a Random Value in the email; and 3. receiving a confirming response utilizing the Random Value. Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed The Random Value SHALL be unique in each email.	Process update and document
3.2.2.4.5	Domain Authorization Document This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.	NA
3.2.2.4.6	Agreed-Upon Change to Website This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.	NA
3.2.2.4.7	DNS Change Confirming the Applicant’s control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a Domain Label that begins with an underscore character. If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after i. 30 days or ii. if the Applicant submitted the Certificate request, the time frame permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).	Process update and document

3.2.2.4.8	IP Address Confirming the Applicant’s control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with Section 3.2.2.5.	
3.2.2.4.9	Test Certificate This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.	NA
3.2.2.4.10	TLS Using a Random Number This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.	NA
3.2.2.4.11	Any Other Method This method has been retired and MUST NOT be used.	NA
3.2.2.4.12	Validating Applicant as a Domain Contact Confirming the Applicant’s control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.	Process update and document
3.2.2.4.13	Email to DNS CAA Contact Confirming the Applicant’s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659, Section 3	Process update and document
3.2.2.4.14	Email to DNS TXT Contact Confirming the Applicant’s control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN. Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated. The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.	

3.2.2.4.15	Phone Contact with Domain Contact Confirm the Applicant’s control over the FQDN by calling the Domain Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. In the event that someone other than a Domain Contact is reached, the CA MAY request to be transferred to the Domain Contact. In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.	
3.2.2.4.16	Phone Contact with DNS TXT Record Phone Contact Confirm the Applicant’s control over the FQDN by calling the DNS TXT Record Phone Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The CA MUST NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation. In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.	
3.2.2.4.17	Phone Contact with DNS CAA Phone Contact Confirm the Applicant’s control over the FQDN by calling the DNS CAA Phone Contact’s phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3. The CA MUST NOT be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation. In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.	

3.2.2.4.18	Agreed-Upon Change to Website v2 Confirming the Applicant’s control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file. 1. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file, and 2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received). The file containing the Request Token or Random Number: A. MUST be located on the Authorization Domain Name, and B. MUST be located under the “/.well-known/pki-validation” directory, and C. 3. MUST be retrieved via either the “http” or “https” scheme, and 4. MUST be accessed over an Authorized Port.	
3.2.2.4.19	Agreed-Upon Change to Website - ACME Confirming the Applicant’s control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555. The following are additive requirements to RFC 8555. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received). The token (as defined in RFC 8555, Section 8.3) MUST NOT be used for more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.	Process update and document
3.2.2.4.20	TLS Using ALPN Confirming the Applicant’s control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737. The following are additive requirements to RFC 8737. The token (as defined in RFC 8737, Section 3) MUST NOT be used for more than 30 days from its creation. The CPS MAY specify a shorter validity period for the token, in which case the CA MUST follow its CPS.	
3.2.2.5	Authentication for an IP Address This section defines the permitted processes and procedures for validating the Applicant’s ownership or control of an IP Address listed in a Certificate. The CA SHALL confirm that prior to issuance, the CA has validated each IP Address listed in the Certificate using at least one of the methods specified in this section.	

3.2.5.1	Agreed-Upon Change to Website Confirming the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by the CA via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request. If a Random Value is used, the CA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of i. 30 days or ii. if the Applicant submitted the certificate request, the time frame permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1 of this document).	Process update and document
3.2.2.5.2	Email, Fax, SMS, or Postal Mail to IP Address Contact Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact. Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.	Process update and document
3.2.2.5.3	Reverse Address Lookup Confirming the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Section 3.2.2.4.	Process update and document
3.2.2.5.4	Using any other method of confirmation, including variations of the methods defined in Section 3.2.2.5, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the IP Address to at least the same level of assurance as the methods previously described in version 1.6.2 of these Requirements. CAs SHALL NOT perform validations using this method after July 31, 2019. Completed validations using this method SHALL NOT be re-used for certificate issuance after July 31, 2019. Any certificate issued prior to August 1, 2019 containing an IP Address that was validated using any method that was permitted under the prior version of this Section 3.2.2.5 MAY continue to be used without revalidation until such certificate naturally expires.	NA
3.2.2.5.5	Phone Contact with IP Address Contact Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. The CA MUST place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call SHALL be made to	Process update and document

	a single number. In the event that someone other than an IP Address Contact is reached, the CA MAY request to be transferred to the IP Address Contact. In the event of reaching voicemail, the CA may leave the Random Value and the IP Address(es) being validated. The Random Value MUST be returned to the CA to approve the request. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.	
3.2.2.5.6	ACME “http-01” method for IP Addresses Confirming the Applicant’s control over the IP Address by performing the procedure documented for an “http-01” challenge in draft 04 of “ACME IP Identifier Validation Extension,” available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.	
3.2.2.5.7	ACME “tls-alpn-01” method for IP Addresses Confirming the Applicant’s control over the IP Address by performing the procedure documented for a “tls-alpn-01” challenge in draft 04 of “ACME IP Identifier Validation Extension,” available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.	
3.2.2.6	Wildcard Domain Validation Before issuing a Wildcard Certificate, the CA MUST establish and follow a documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate is “registry-controlled” or is a “public suffix” (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation). If the FQDN portion of any Wildcard Domain Name is “registry-controlled” or is a “public suffix”, CAs MUST refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue “*.co.uk” or “*.local”, but MAY issue “*.example.com” to Example Co.). Determination of what is “registry-controlled” versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a “public suffix list” such as the Public Suffix List (PSL), and to retrieve a fresh copy regularly. If using the PSL, a CA SHOULD consult the “ICANN DOMAINS” section only, not the “PRIVATE DOMAINS” section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the “ICANN DOMAINS” section. A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.	
3.2.2.7	Data Source Accuracy Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA SHOULD consider the following during its evaluation: 1. The age of the information provided, 2. The	Process update and document

	frequency of updates to the information source, 3. The data provider and purpose of the data collection, 4. The public accessibility of the data availability, and 5. The relative difficulty in falsifying or altering the data. Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.	
3.2.2.8	CAA Records As part of the Certificate issuance process, the CA MUST retrieve and process CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an Onion Domain Name. If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater. This stipulation does not prevent the CA from checking CAA records at any other time. When processing CAA records, CAs MUST process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. CAs MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.	
3.2.5	Validation of authority If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative’s certificate request.	
3.2.6	Criteria for Interoperation or Certification The CA SHALL disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).	
3.3.2	Identification and authentication for re-key after revocation. When current Signing Key is used for identification and authentication purposes, the life of the new certificate shall not exceed beyond the initial identity-proofing times specified in the table above.	
4.1	Certificate Application	
4.1.1	Who can submit a certificate application	NA
4.1.2	Enrolment process and responsibilities Prior to the issuance of a Certificate, the CA SHALL obtain the following documentation from the Applicant: 1. A certificate request, which may be electronic; and	Process update and document

	2. An executed Subscriber Agreement or Terms of Use, which may be electronic. The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements. Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 4.2.1, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically. The certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.	
4.2	Certificate application processing	
4.2.1	Performing identification and authentication functions The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.	Process update and document
4.2.2	Approval or rejection of certificate applications CAs SHALL NOT issue Certificates containing Internal Names or Reserved IP Addresses	
4.2.3	Time to process certificate applications	
4.9.1	Reasons for Revoking a Subscriber Certificate 1. The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs: 2. The Subscriber requests in writing that the CA revoke the Certificate; 3. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; 4. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; 5. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); 6. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.	Process update and document

	a. The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following occurs: 7. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6; 8. The CA obtains evidence that the Certificate was misused; 9. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use; 10. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant’s right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); 11. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; 12. The CA is made aware of a material change in the information contained in the Certificate; 13. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA’s Certificate Policy or Certification Practice Statement; 14. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate; 15. The CA’s right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; 16. Revocation is required by the CA’s Certificate Policy and/or Certification Practice Statement; or The CA is made aware of a demonstrated or proven method that exposes the Subscriber’s Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.	
4.9.1.2	Reasons for Revoking a Subordinate CA Certificate The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs: a. The Subordinate CA requests revocation in writing; b. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization; c. The Issuing CA obtains evidence that the Subordinate CA’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6; d. The Issuing CA obtains evidence that the Certificate was misused;	

	e. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement; f. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading; g. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; 8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or	
4.9.2	Who can request revocation The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.	Update RA portal, Process and document
4.9.3	Procedure for revocation request The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports. The CA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA SHALL publicly disclose the instructions through a readily accessible online means and in Section 1.5.2 of their CPS.	Process update and document

4.9.4	Revocation request grace period	NA
4.9.5	Time within which CA must process the revocation request Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report. After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1. The date selected by the CA SHOULD consider the following criteria: 1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm); 2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties); 3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber; 4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and 5. Relevant legislation.	Process update and document
4.9.6	Revocation checking requirement for relying parties	NA
4.9.7	CRL issuance frequency (if applicable) For the status of Subscriber Certificates: If the CA publishes a CRL, then the CA SHALL update and reissue CRLs at least once every seven days, and the value of the next Update field MUST NOT be more than ten days beyond the value of the this Update field. For the status of Subordinate CA Certificates: The CA SHALL update and reissue CRLs at least: I. once every twelve months; and within 24 hours after revoking a Subordinate CA Certificate. The value of the next Update field MUST NOT be more than twelve months beyond the value of the this Update field.	Process update and document
4.9.8	Maximum latency for CRLs (if applicable)	

4.9.9	On-line revocation/status checking availability 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	Change in CPS document
4.9.10	On-line revocation checking requirements OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019. The validity interval of an OCSP response is the difference in time between the this Update and next Update field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds. For the status of Subscriber Certificates: 1. OCSP responses MUST have a validity interval greater than or equal to eight hours; 2. OCSP responses MUST have a validity interval less than or equal to ten days; 3. For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate. 4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate. For the status of Subordinate CA Certificates: The CA SHALL update information provided via an Online Certificate Status Protocol i. at least every twelve months; and ii. within 24 hours after revoking a Subordinate CA Certificate. If the OCSP responder receives a request for the status of a certificate serial number that is “unused”, then the responder SHOULD NOT respond with a “good” status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5, the responder MUST NOT respond with a “good” status for such requests. The CA SHOULD monitor the OCSP responder for requests for “unused” serial numbers as part of its security response procedures. The OCSP responder MAY provide definitive responses about “reserved” certificate serial numbers, as if there was a corresponding Certificate that matches the Pre	Process update and document

	certificate [RFC6962]. A certificate serial number within an OCSP request is one of the following three options: a. “assigned” if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or b. “reserved” if a Pre certificate [RFC6962] with that serial number has been issued by a. the Issuing CA; or b. a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or “unused” if neither of the previous conditions are met.	
4.9.11	Other forms of revocation advertisements available	NA
4.9.12	Special requirements re key compromise See Section 4.9.1.	NA
4.9.13	Circumstances for suspension The Repository MUST NOT include entries that indicate that a Certificate is suspended.	NA
4.9.14	Who can request suspension	NA
4.9.15	Procedure for suspension request	Process update and document
4.9.16	Limits on suspension period.	Process update and document
5.3.5	Job rotation frequency and sequence	Process update and document
5.3.6	Sanctions for unauthorized actions	
5.3.7	Independent Contractor Controls The CA SHALL verify that the Delegated Third Party’s personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.	
5.3.8	Documentation supplied to personnel	
5.4.2	Frequency of processing audit log	Process update and document

5.4.3	Retention period for audit log The CA and each Delegated Third Party SHALL retain, for at least two (2) years: 1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of: a. the destruction of the CA Private Key; or b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key; 2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the expiration of the Subscriber Certificate; 3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred. Note: While these Requirements set the minimum retention period, the CA MAY choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past audit log events.	Process update and document
5.4.4	Protection of audit log	
5.4.5	Audit log backup procedures	
5.4.6	Audit collection System (internal vs. external)	Process update and document
5.4.7	Notification to event-causing subject	
5.4.8	Vulnerability assessments Additionally, the CA's security program MUST include an annual Risk Assessment that: 1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes; 2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and 3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.	Process update and document
5.5	Records archival	

5.5.1	Types of records archived The CA and each Delegated Third Party SHALL archive all audit logs (as set forth in Section 5.4.1). Additionally, the CA and each Delegated Third Party SHALL archive: 1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and 2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.	Process update and document
5.5.2	Retention period for archive Archived audit logs (as set forth in Section 5.5.1 SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer. Additionally, the CA and each Delegated Third Party SHALL retain, for at least two (2) years: 1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1); and 2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of: 1. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or 2. the expiration of the Subscriber Certificates relying upon such records and documentation.	Process update and document
5.5.3	Protection of archive	Provide reference in CCA checklist
5.5.4	Archive backup procedures	Provide reference in CCA checklist
5.5.5	Requirements for time-stamping of records	
5.5.6	Archive collection system (internal or external)	
5.5.7	Procedures to obtain and verify archive information	
6.1.1.2	RA Key Pair Generation	

6.1.2	Private key delivery to subscriber Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key without authorization by the Subscriber. If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.	
6.1.3	Public key delivery to certificate issuer	
6.1.4	CA public key delivery to relying parties	
6.1.5	Key sizes For RSA key pairs the CA SHALL: • Ensure that the modulus size, when encoded, is at least 2048 bits, and; • Ensure that the modulus size, in bits, is evenly divisible by 8. For ECDSA key pairs, the CA SHALL: • Ensure that the key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve. No other algorithms or key sizes are permitted.	
6.1.6	Public key parameters generation and quality checking RSA: The CA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16 + 1 and 2^256 - 1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89] ECDSA: The CA SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]	
6.2.9	Deactivating Private Keys	Provide reference in CCA checklist
6.2.10	Destroying Private Keys	
6.5.1	Specific computer security technical requirements The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance	

6.5.2	Computer security rating	
6.6	Life cycle technical controls	
6.6.1	System development controls	Process update and document
6.6.2	Security management controls	
6.6.3	Life cycle security controls	
8.7	Self-Audits	
8.7	Self-Audits During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.4, the CA SHALL strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. The CA SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement. The CA SHALL internally audit each Delegated Third Party's compliance with these Requirements on an annual basis. During the period in which a Technically Constrained Subordinate CA issues Certificates, the CA which signed the Subordinate CA SHALL monitor adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practice Statement. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the CA shall ensure all applicable CP are met.	Process update and document