CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Webtrust® for Certification Authorities

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES

Release Date 1 June 2021

Effective Date For engagement periods commencing on or after 1 June 2021

Version 2.2.2

Document History

Version	Publication Date	Revision Summary
1.0	July 2000	Initial release
2.0	March 2011	Updated criteria release
2.1	1 September 2017	Updated introduction section, including clarifying definitions for Root CA, Intermediate/Issuing CA, and Subordinate CA, and adding explanation of a Bridge CA structure Removed references to WebTrust v1 for Business Practices Disclosures. All CP and CPS documents must now be structured in accordance with RFC 3647 (recommended) or RFC 2527.Updated the following criteria: • Criteria 1.1 and 1.2 – removed WebTrust v1 references • Criteria 2.1 and 2.2 – swapped order to be consistent with 1.1 and 1.2 • Criterion 3.6 – Expanded scope to specifically address hypervisors and network devices • Criterion 3.7 – Expanded scope to specifically address system patching and change management activities • Criterion 3.8 – Clarified scope to include requirement for backups of CA information and data to be taken at regular intervals in accordance with the CA's disclosed business practices. • Criterion 4.5 – Split into two criteria (4.5 and 4.6), subsequent criteria renumbered • Criterion 4.6 – Clarified scope to include destruction of any copies of CA keys for any purpose, and added illustrative controls addressing formal key destruction ceremonies. • Criterion 4.10 – New criterion added to address CA Key Transportation events • Criterion 4.11 – New criterion added to address CA Key Migration events • Criterion 6.1 – Streamlined criteria, minor updates to illustrative controls • Criterion 7.1 – Updated to address cross certificate requests

Version	Publication Date	Revision Summary
2.2	1 May 2019	Minor updates made to conform to ISO 21188:2018 Edition
2.2.1	1 November 2020	Correct typographical errors and general clean-up. No substantive change in content.
2.2.2	1 June 2021	Inclusion of footnote for principle one setting out disclosure requirements.

Acknowledgements

This document has been prepared by the WebTrust/PKI Assurance Task Force (the "Task Force") for use by those practitioners enrolled by CPA Canada to perform WebTrust for Certification Authorities engagements.

Members of the Task Force are:

- Jeffrey Ward, BDO USA, LLP (Chair)
- Donald E. Sheehy (Vice-Chair)
- Chris Czajczyc, Deloitte LLP
- David Roque, Ernst & Young LLP
- Zain Shabbir, KPMG LLP

Significant support has been provided by:

- Timothy Crawford, BDO USA, LLP
- Daniel J. Adam, Deloitte & Touche LLP
- Donoghue Clarke, Ernst & Young LLP
- Eric Lin, Ernst & Young LLP

CPA Canada Support

- Kaylynn Pippo, Principal, Research, Guidance and Support
- Gord Beal, Vice President, Research, Guidance and Support
- Janet Treasure, Vice President, Member Development and Support
- Bryan Walker, Consultant

Table of Contents

Introduction

Introduction to WebTrust Principles and Criteria for Certification Authorities Version 2.2.2

This document provides a framework for practitioners to assess the adequacy and effectiveness of the controls used by Certification Authorities (CAs). As a result of the technical nature of the activities involved in the application of PKI technology to, among other businesses, securing ecommerce transactions, this document also provides a brief overview of public key infrastructure (PKI) using cryptography and trusted third party concepts.

This document replaces version 2.2.1 of the WebTrust Principles and Criteria for Certification Authorities that was issued in November 2020, and like version 2.2.1, is substantially based on ISO 21188 "Public Key Policy and Practices Framework".

The public accounting profession has continued to play its role, with an intent to increase confidence in the application of PKI technology, by establishing a basis for providing third party assurance to the assertions made by CAs. Although these Principles and Criteria are intended to be used in the conduct of WebTrust engagements by those practitioners enrolled by CPA Canada., this document can be used, in conjunction with consideration of the additional compliance requirements set forth by the CA/Browser Forum for publicly-trusted CAs (i.e., Baseline Requirements, Network Security Requirements, Code Signing, Extended Validation, etc.) in the conduct of any assurance engagements or internal audits for Public PKIs.

These Principles and Criteria also represent an effective benchmark for CAs to conduct control self-assessments for enterprise and private PKIs.

Input was also obtained from the Certification Authority Browser Forum (CA/Browser Forum – see www.cabforum.org) for the content and control activities added in version 2.2.1 of this framework. The CA/Browser Forum was formed among certification authorities (CAs) and vendors of Internet browser software and other applications. This voluntary organization has worked collaboratively in defining guidelines and means of implementation for PKI as used on the Internet and in certain applications.

These Principles and Criteria continue to be consistent with standards developed by the American National Standards Institute (ANSI), International Organization for Standardization (ISO), and Internet Engineering Task Force (IETF).

Effective Date

These Principles and Criteria are effective for engagement periods commencing on or after 1 June 2021. Earlier adoption is permitted and encouraged.

Importance of PKI

PKI provides a means for relying parties (meaning, recipients of certificates who rely on those certificates and/or digital signatures verified using those certificates) to know that another individual's or entity's public key actually belongs to that individual/entity. CA organizations and/or CA functions have been established to address this need.

Cryptography is critical to establishing secure communications and transactions. However, it must be coupled with other secure protocols in order to provide a comprehensive security solution. Several cryptographic protocols require digital certificates (in effect, electronic credentials) issued by an independent trusted third party (the CA) to authenticate the transaction. CAs have assumed an increasingly important role in providing this security. Although there is a large body of existing national, international, and proprietary standards and guidelines for the use of cryptography, the management of digital certificates, and the policies and practices of CAs, these standards have not been applied or implemented uniformly.

This version is titled the WebTrust Principles and Criteria for Certification Authorities Version 2.2.2. These Principles and Criteria are intended to address user (meaning, subscriber and relying party) needs and concerns and are designed to benefit users and providers of CA services by providing a common body of knowledge that is communicated to such parties.

Overview

What Is a Public Key Infrastructure?

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. PKI facilitates the secure electronic transfer of information for a range of network activities including, but not limited to, e-commerce, internet banking and confidential email. PKI enables parties to identify one another by providing authentication with digital certificates, and allows reliable business communications by providing confidentiality through the use of encryption, and authentication data integrity and a reasonable basis for nonrepudiation through the use of digital signatures.

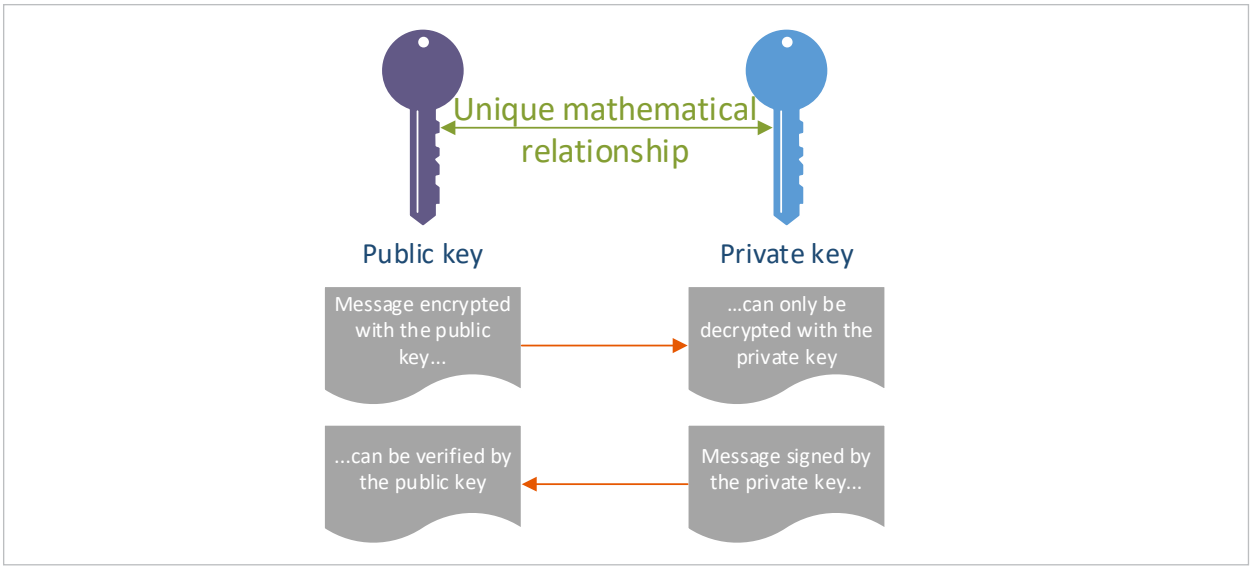
PKI uses public / private-key pairs – two mathematically related keys. Typically, one of these keys is made public, by posting it on the Internet for example, while the other remains private. Public-key cryptography works in such a way that a message encrypted with the public key can only be decrypted with the private key, and, conversely, a message signed with a private key can be verified with the public key. This technology can be used in different ways to provide the four ingredients required for trust, namely: confidentiality, authentication, integrity, and nonrepudiation.

Using PKI, a subscriber (meaning an end entity (or individual) whose public key is cryptographically bound to his or her identity in a digital certificate) has an asymmetric cryptographic key pair (meaning a public key and a private key). The subscriber's private key must be kept secret, whereas the public key may be made widely available, usually presented in the form of a digital certificate to ensure that relying parties know with confidence the identity to which the public key belongs. Using public key cryptography, the subscriber could send a message signed with his or her private key. The signature can be validated by the message recipient using the subscriber's public key. The subscriber could also encrypt a message using the recipient's public key. The message can be decrypted only with the recipient's private key.

A subscriber first obtains a public / private key pair (generated by the subscriber or for the subscriber as a service). The subscriber then goes through a registration process by submitting their public key to a Certification Authority or a Registration Authority (RA), which acts as an agent for the CA. The CA or RA verifies the identity of the subscriber in accordance with the CA's established business practices (that may be contained in a Certification Practice Statement), and then issues a digital certificate. The certificate includes the subscriber's public key and identity information, and is digitally signed by the CA, which binds the subscriber's identity to that public key. The CA also manages the subscriber's digital certificate through the certificate life cycle (meaning, from registration

through revocation or expiration). In some circumstances, it remains important to manage digital certificates even after expiry or revocation so that digital signatures on stored documents held past the revocation or expiry period can be validated at a later date.

The following diagram illustrates the relationship between a subscriber's public and private keys, and how they are used to secure messages sent to a relying party:



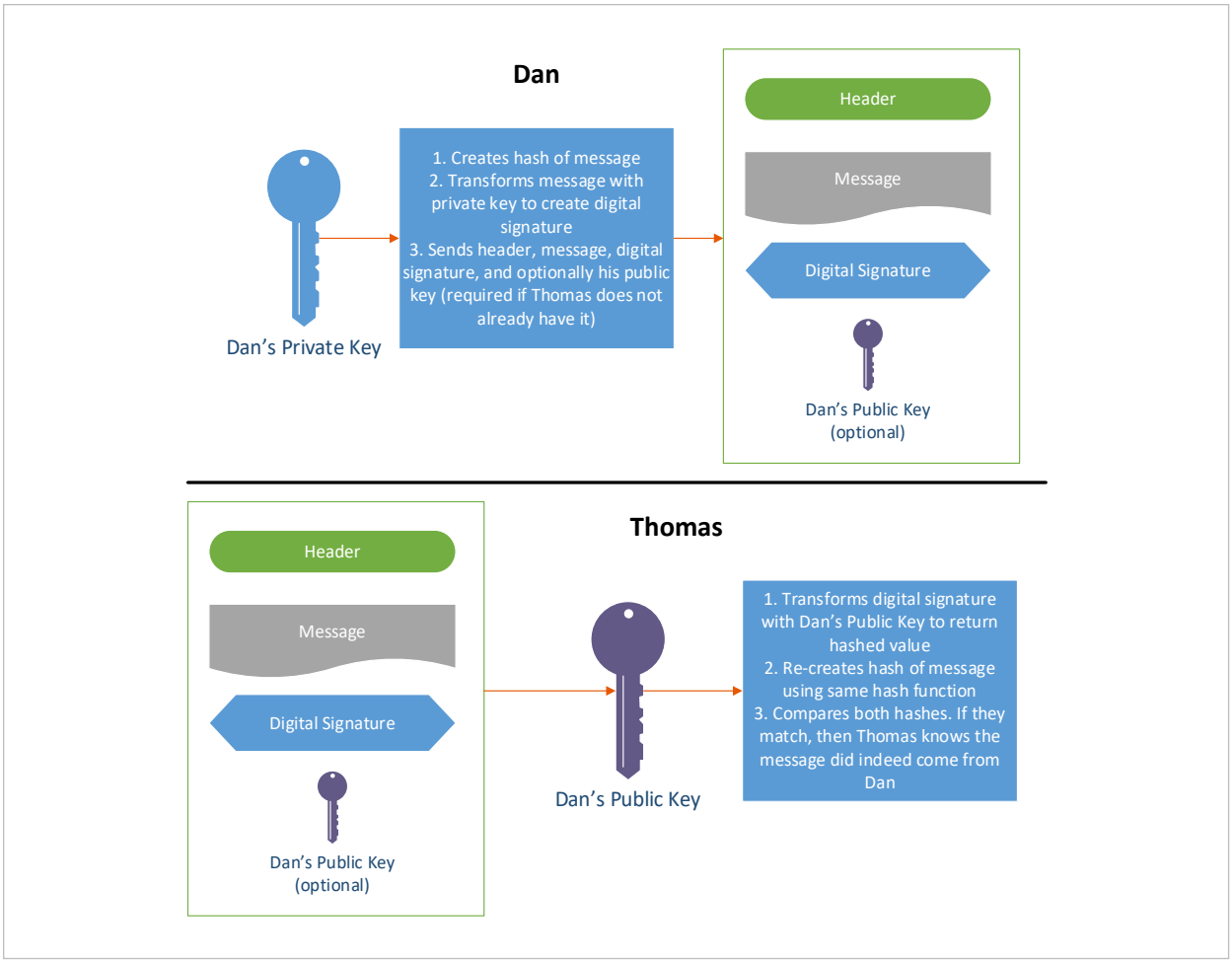
For example, a transaction submitted by a customer to an online merchant via the Internet can be encrypted with the merchant's public key and therefore can only be decrypted by that merchant using the merchant's private key – ensuring a level of confidentiality. Confidentiality can also be achieved through the use of other protocols such as Secure Socket Layer/Transport Layer Security (SSL/TLS) and Secure/Multipurpose Internet Mail Extensions (S/MIME) that often operate together with PKI.

What Is a Digital Signature?

Digital signatures are a mathematical technique that can be used to provide authentication, integrity, and nonrepudiation for various digital items including a message, document, or software code. Generally speaking, if Claire sends a digitally signed message to Sally, Claire's private key is used to generate the digital signature and her public key can be used by Sally to verify the signature. The mathematical processes employed are somewhat different depending on the kind of asymmetric cryptographic algorithm employed. For example, the processes are slightly different for reversible algorithms (i.e., those which can be readily used to support digital signatures as well as encryption) such as Rivest Shamir Adleman (RSA) and irreversible algorithms such as the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA).

The following example illustrates the digital signature generation and verification process for a reversible asymmetric cryptographic algorithm (such as RSA). Suppose Dan wants to send a digitally signed message to Thomas. Dan runs the message through a hash function (meaning, a mathematical function that converts a message into a fixed length block of data, the hash, in a fashion such that the hash uniquely reflects the message – in effect, it is the message's "fingerprint"). Dan then transforms the hash using the algorithm and his private key to create the digital signature which is appended to the message. A header is also appended to the message, indicating Thomas' email address, Dan's email address, and other information such as the time the message is sent. The message header, the message itself, and the digital signature are then sent to Thomas. Dan can optionally send his public key certificate to Thomas in the message itself. All of this is usually done by the e-mail software in such a way that the process is transparent to the user.

The following diagram illustrates the process of using Dan's key pair to ensure the integrity and authenticity of a message sent by Dan to Thomas:



To determine whether the message came from Dan (meaning, authentication) and to determine whether the message has not been modified (meaning, integrity), Thomas validates the digital signature. To do so, Thomas must obtain Dan's public key certificate. If Dan did not send his public key certificate as part of the message, Thomas would typically obtain Dan's public key certificate from an online repository (maintained by the CA or another party acting as the agent of the CA, or any other source even if unrelated to the CA). Thomas then validates that Dan's digital certificate (containing his public key) was signed by a recognised Certification Authority to ensure that the binding between the public key and Dan as represented in the certificate has not been altered. Next, Thomas extracts the public key from the certificate and uses that public key to transform the digital signature to reveal the original hash. Thomas then runs the message as received through the same hash function to create a hash of the received message. To verify the digital signature, Thomas compares these two hashes. If they match, then the digital signature validates and Thomas knows that the message came from Dan and it was not modified from the time the signature was made. If the hashes do not match, then Thomas knows that the message was either modified in transit or the message was not signed with Dan's private key. As a result, Thomas cannot rely on the digital signature.

Digital signatures can also be used to provide a basis for nonrepudiation so that the signer cannot readily deny having signed the message. For example, an online brokerage customer who purchases one thousand shares of stock using a digitally signed order via the Internet should have a difficult task if he or she later tries to deny (meaning, repudiate) having authorised the purchase.

What Are the Differences Between Encryption Key Pairs and Signing Key Pairs?

Establishing a reasonable basis for nonrepudiation requires that the private key used to create a digital signature (meaning, the signing private key) be generated and stored securely under the sole control of the user. In the event a user forgets his or her password or loses, breaks, or destroys his/her signing private key, it is acceptable to generate a new signing key pair for use from that point forward with minimal impact to the subscriber. Previously signed documents can still be verified with the user's old signature verification public key. Documents subsequently signed with the user's new signing private key must be verified with the user's new signature verification public key.

Extra care is required to secure the Certification Authority's signing private key, which is used for signing user certificates. The trustworthiness of all certificates issued by a CA depends upon the CA's protecting its private signing key. CAs securely back up their private signing key(s) for business continuity purposes to allow the CA to continue to operate in the event that the CA's private signing key is accidentally destroyed (but not compromised) as a result of hardware failure, for example. Except for CA business continuity purposes,

there are generally no technical or business reasons to back up a signing private key. The leading practice is for a CA's private signing key to be protected in a properly secured Hardware Security Module (HSM) deployed and maintained in compliance with leading security practices.

On the other hand, it is often desirable that a key pair used for encryption and decryption be securely backed up to ensure that encrypted data can be recovered when a user forgets his or her password or otherwise loses access to his or her decryption key. This is analogous to requiring that the combination to a safe be backed up in case the user forgets it, or becomes incapacitated. As a result, a PKI typically requires two key pairs for each user: one key pair for encryption and decryption and a second key pair for signing and signature verification.

What Is a Certification Authority?

In order for these technologies to enable parties to securely communicate, one important question must be answered. How will we know in the digital world that an individual's public key actually belongs to that individual? A digital certificate, which is an electronic document containing information about an individual and his or her public key, is the answer. This document is digitally signed by a trusted organisation referred to as a Certification Authority (CA). The basic premise is that the CA is vouching for the link between an individual's identity and his or her public key. The Certification Authority provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate. The digital signature placed on the public key certificate by the CA provides the cryptographic binding between the entity's public key, the entity's name, and other information in the certificate, such as a validity period. For a relying party to determine whether the certificate was issued by a legitimate CA, the relying party must verify the issuing CA's signature on the certificate. The public keys of many common Root CAs (as later defined) are pre-loaded into standard desktop and mobile operating systems, and Web browsers (for example: Apple macOS, iOS, and Safari, Google Android and Chrome, Microsoft Windows and Internet Explorer, and Edge, Mozilla Firefox, etc.). In the enterprise, a company may choose to provision users' devices with additional Root CA certificates for its own internal PKI, or the PKI's of trusted third parties. This allows the relying party to verify the issuing CA's signature using the CA's public key to determine whether the certificate was issued by a trusted CA.

The purpose of a CA is to manage the certificate life cycle, which includes generation and issuance, distribution, renewal and rekey, revocation, and suspension of certificates. In some cases, the CA delegates the initial registration of subscribers to Registration Authorities (RAs) that act as agents for the CA. In others, the CA also acts as the RA and may perform registration functions directly. The CA is also responsible for providing certificate status information through the issuance of Certificate Revocation Lists (CRLs) and/or the

maintenance of an online status checking mechanism such as the Online Certificate Status Protocol (OSCP). Typically, the CA posts the certificates and CRLs that it has issued to a repository (such as an online directory) which is accessible to relying parties.

What Is a Registration Authority?

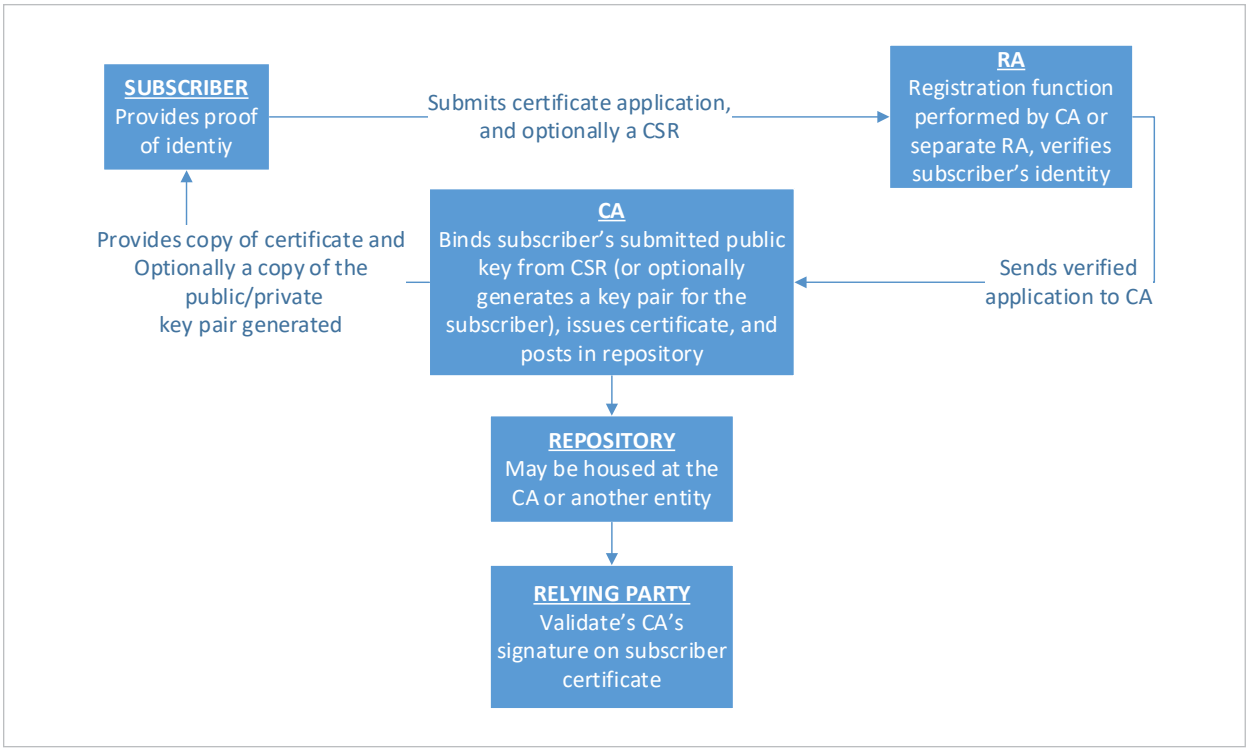
A Registration Authority (RA) is an entity that is responsible for the identification and authentication of subscribers, but does not sign or issue certificates. In some cases, the CA performs the subscriber registration function internally. In other cases, the CA might delegate the RA function to external registration authorities (sometimes referred to as Local Registration Authorities or LRAs) that may or may not be part of the same legal entity as the CA. In still other cases, a customer of a CA may arrange with that CA to perform the RA function itself or use its agent.

The initial registration process for a subscriber is as follows, though the steps may vary from CA to CA and will also depend upon the Certificate Policy under which the certificate is to be issued. The subscriber first generates his or her own public / private key pair, which is submitted to the CA as part of the Certificate Signing Request (CSR). The CSR contains the subscriber's public key and is signed with its private key allowing the CA to verify that the subscriber is indeed in possession of the private key. (In some implementations, a CA may generate the subscriber's key pair and securely deliver it to the subscriber, but this is normally done only for encryption key pairs, not signature key pairs.) Then the subscriber produces proof of identity in accordance with the applicable Certificate Policy requirements and demonstrates that he or she holds the private key corresponding to the public key without disclosing the private key (typically by digitally signing a piece of data with the private key, with the subscriber's digital signature then verified by the CA). Once the association between a person and a public key is verified, the CA issues a certificate. The CA digitally signs each certificate that it issues with its private key to provide the means for establishing authenticity and integrity of the certificate.

The CA then notifies the subscriber of certificate issuance and gives the subscriber an opportunity to review the contents of the certificate before it is made public. Assuming the subscriber approves the accuracy of the certificate, the subscriber will publish the certificate and/or have the CA publish it and make it available to other users. A repository is an electronic certificate database that is available online. The repository may be maintained by the CA or a third party contracted for that purpose, or by the subscriber, or by any other party. Subscribers may obtain certificates of other subscribers and certificate status information from the repository. For example, if a subscriber's certificate was revoked, the repository would indicate that the subscriber's certificate has been revoked and should not be relied upon. The ability to update the repository is typically retained by the CA. Subscribers and other relying parties would have read-only access to the repository.

Because the certificates stored in the repository are digitally signed by the CA, they cannot be maliciously changed without detection, even if someone were to hack into the repository.

The following diagram illustrates the relationship between the subscriber and the RA and CA functions:



Types of RAs Today

There are various types of RAs that are currently in existence. RAs can be either internal or external. They can be operated by the same entity as the CA, can be independent of the CA (performing authentication processes for a number of customers of the CA), or be constrained so that that are only authorized to perform RA functions within a specific scope (normally for one customer of the CA). In addition, for WebPKI, an Enterprise RA is a type of constrained RA, where another RA delegates a specific domain namespace or directory subtree to the constrained RA. For example, Example Corp. owns example.com and designates their IT Security team as the Enterprise RA for dNSName:example.com and O=Example Corp, L=Springfield, C=US.

What Is the Impact of an Internal RA?

In performing a WebTrust for Certification Authorities engagement, the practitioner will consider how the CA handles the RA function and whether the RA function is within the scope of the examination. Where an internal RA exists (or operated by the same entity as the CA) it should be included in the WebTrust for Certification Authorities engagement.

What Is the Impact of an External Constrained RA?

External registration authorities are normally required to comply with the relevant provisions of the CA's business practices disclosures, often documented in a Certification Practice Statement and applicable Certificate Policy(s). In performing a WebTrust for Certification Authorities engagement, the practitioner must consider how the CA handles the RA function. Let's take an example of a CA that provides CA services to several banks, and delegates the subscriber registration function to RAs that are specifically designated functional groups within each bank. Where a constrained RA relationship exists, the functions performed by these specific groups would typically be outside the scope of the WebTrust for Certification Authorities examination performed for the CA. It would also normally not require a separate RA engagement.

What Is the Impact of an External Unconstrained RA?

External unconstrained registration authorities are normally required to comply with the relevant provisions of the CA's business practices disclosures, often documented in a Certification Practice Statement and applicable Certificate Policy(s). These RAs are important to the CAs certificate issuance process, especially in regard to Extended Validation, where the validation process is more extensive. There is an expectation that the entire hierarchy for the CA is subject to third party assurance, including RAs. RAs are, however, not part of the WebTrust for CA engagement of the CA since they are separate entities not controlled by the CA. External RAs could be examined and reported upon separately from the CA, using the relevant criteria contained in WebTrust Principles and Criteria for Registration Authorities.

What Is a Certificate Policy and a Certification Practices Statement?

A Certificate Policy (CP) is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements, and describes the boundaries and acceptable uses of certificates from a given PKI. A CP may apply to the entire trust chain down (i.e., from the Root CA all the way down to the end-entity or 'leaf' certificates), or there may be multiple CPs each governing a different hierarchal branch of the PKI (i.e., one CP addressing server authentication certificates and one addressing secure email certificates).

A Certification Practice Statement (CPS) is a statement of the practices which a Certification Authority employs in issuing and managing certificates. The CPS describes in more detail how a CA implements a given Certificate Policy, and cannot contradict what is stated in the CP. For example, if a CP states that only S/MIME certificates for Secure Email are to be issued, the corresponding CPS cannot then say that SSL/TLS server authentication certificates are issued.

Together, the CP and CPS represent a CA's business practice disclosures. It is leading practice for the CP at a minimum be publicly available to relying parties, and most CAs also make their CPS publicly available. Many CAs also publish a combined CP/CPS document instead of maintaining two separate documents.

CA Models

CAs may be linked using different architectures depending on the PKI's specific uses. Three common examples are:

1. Standard hierarchical
2. Cross-certified (shared trust); and
3. Bridging.

Differences between Root CAs, intermediate / issuing CAs, and subordinate CAs

A **Root CA** is the top-level of a given PKI, and represents the 'trust anchor' for the chain of trust. Root CA certificates are generally self-signed (i.e., the Root CA signs a certificate that names itself as the certificate subject). Major operating system and browser vendors embed and distribute the Root CA certificates for many public CAs, and enterprises may add to these by distributing the Root CA certificates of internal PKIs to their users. As applications will trust any valid certificate that chains up to a Root CA that is in its trust store, extra precautions to protect the integrity of the Root CA and its private signing key must be taken. It is leading practice for Root CAs to be 'offline' and/or 'air gapped' from other networks, and only brought online in a controlled environment to issue certificates to other intermediate / issuing CAs, subordinate CAs, cross-certificates, and CRLs.

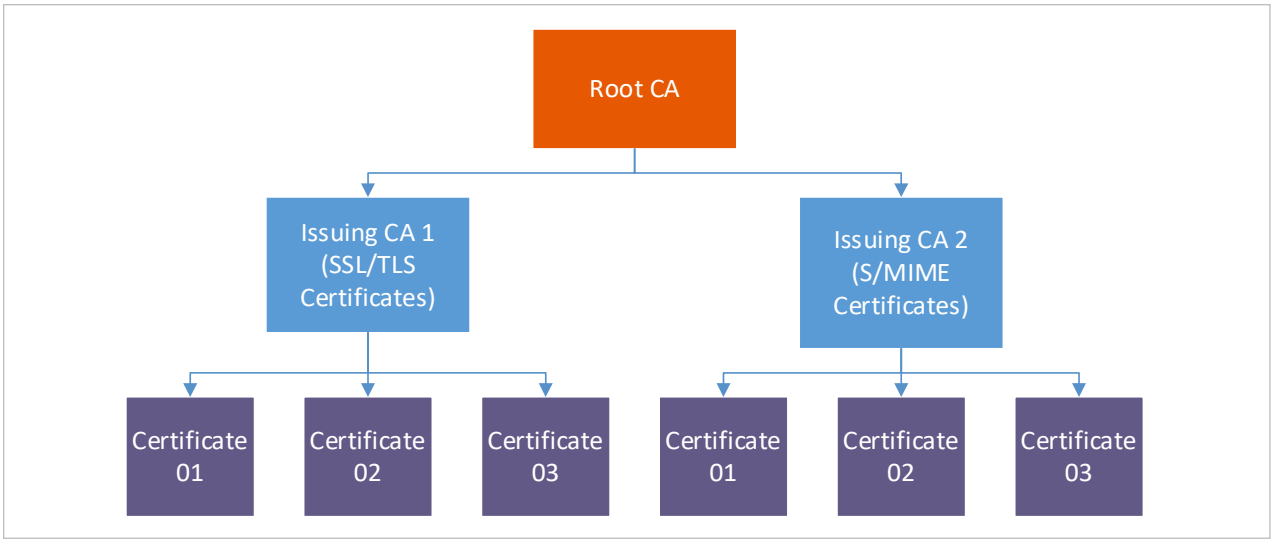
An **Intermediate** or **Issuing CA** is a CA that falls below the Root CA in a given PKI and are normally managed by the same entity as the Root CA. Common practice is for the one or more Intermediate / Issuing CAs to be chained off a specific Root CA, and operate in an online environment to issue certificates and publish revocation information to users. In some cases, an Intermediate CA may also operate offline (similar to a Root CA) and issue certificates to online issuing CAs underneath it. This approach is often taken to segregate the PKI into different hierarchical chains based on policy.

A **Subordinate CA** is similar to an Intermediate or Issuing CA in that it also chains off of the Root CA, however the distinction is that a Subordinate CA is generally operated by a different party than the Root or Intermediate CA above it[1]. Subordinate CA relationships are created by a Root or Intermediate CA directly signing the certificate for the Subordinate. Issuing a cross-certificate to a CA in a different PKI also creates a Subordinate CA relationship. As externally operated Subordinate CAs are operated by a different party, additional care may be required to protect relying parties, and Subordinate CA certificates may be issued with extensions that limit their scope, path length, and valid certificate types.

Standard hierarchical model

In a hierarchical model, a highest level (or Root) CA is deployed and various Intermediate CAs may be set up for various business units, domains or communities of interest. The Root CA validates the intermediate CAs, which in turn issue certificates to lower tier CAs or directly to subscribers. Such a Root CA typically has more stringent security requirements than an Intermediate CA. Although it is difficult for an attacker to access the Root CA (which in some implementations is only online in the rare event that it must issue, renew, or revoke Intermediate or Subordinate CA certificates and publish revocation status information), one drawback to this model is that the Root CA represents a single point of failure. In the hierarchical model, the Root CA maintains the established "community of trust" by ensuring that each entity in the hierarchy conforms to a minimum set of practices. Adherence to the established policies may be tested through assurance engagements of the Intermediate and Subordinate CAs and, in a number of cases, the Registration Authorities.

The following diagram illustrates the structure and relationships between certification authorities and subscribers operating in a two-level hierarchical model:

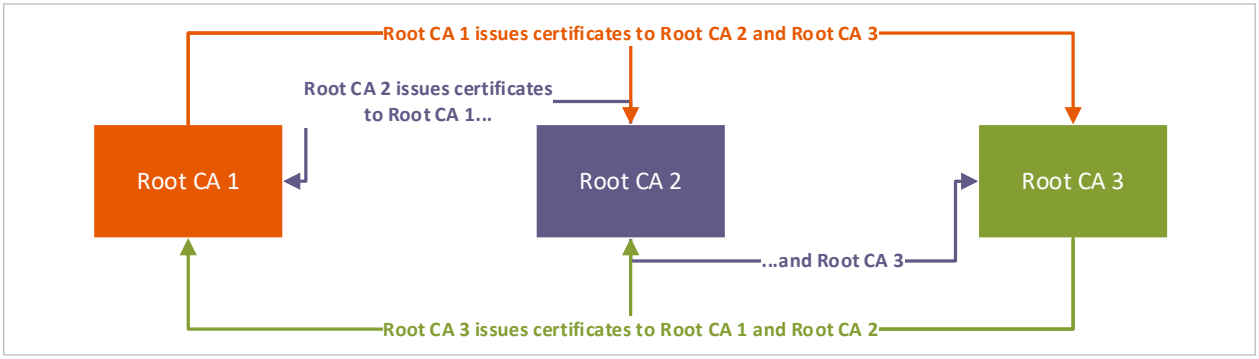


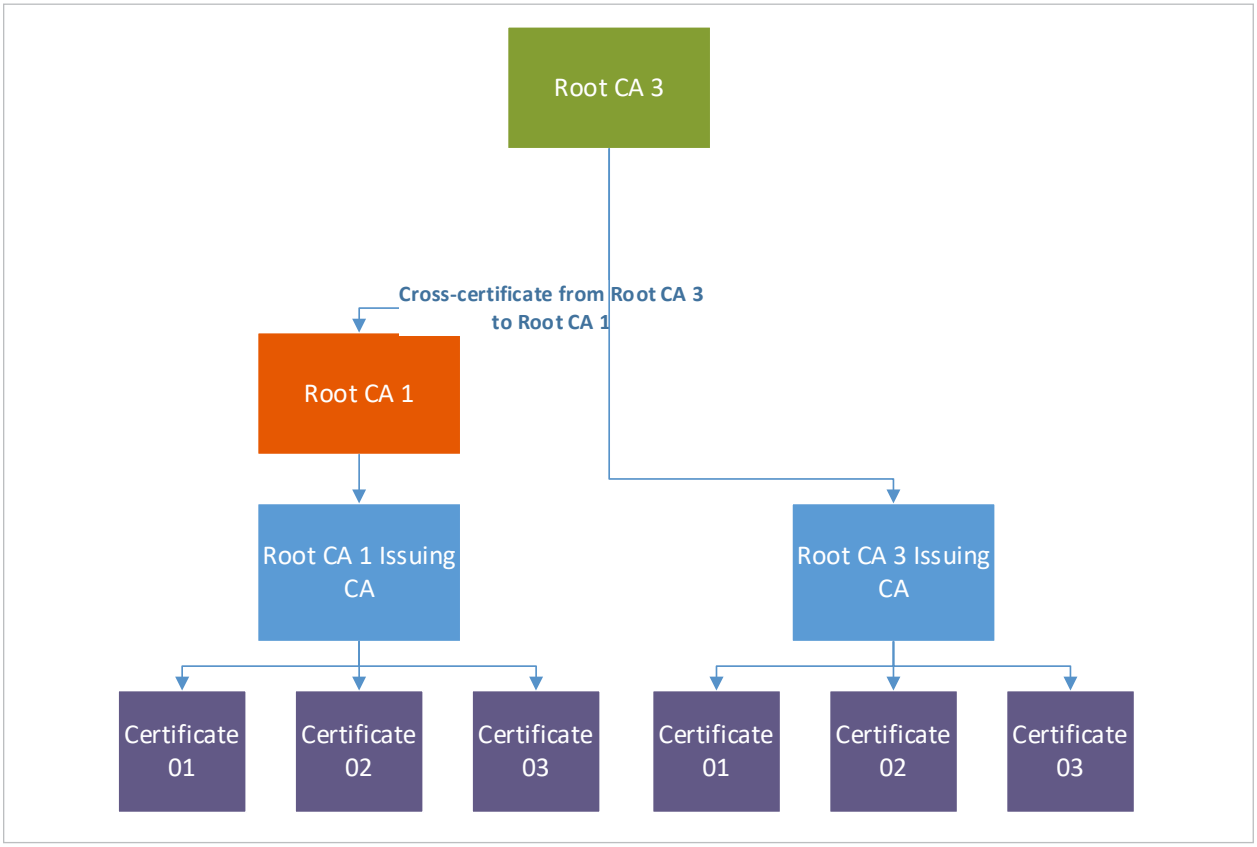
1 The term Subordinate CA may be used in some cases to refer to any CA that chains off a Root CA, regardless of affiliation. However, for the purposes of these WebTrust Principles and Criteria for Certification Authorities, Subordinate CA distinctly refers to those CAs that are operated by a different party than the CA above it.

Cross-certified model

In a cross-certified model, the Root CAs from one or more PKIs issue certificates naming each other as the subject. This allows for trust to be established across separate PKIs when relying parties may only have one of the Root CAs in their trust store.

For example, if Root CA 1 issues certificates to Root CA 2 and Root CA 3, Root CA 2 issues certificates to Root CA 1 and Root CA 3, and Root CA 3 issues certificates to Root CA 1 and Root CA 2, a relying party which only has one of the Root CAs in their trust store (say Root CA 3), will trust all certificates from each of these PKIs because they will eventually chain up to Root CA 3:



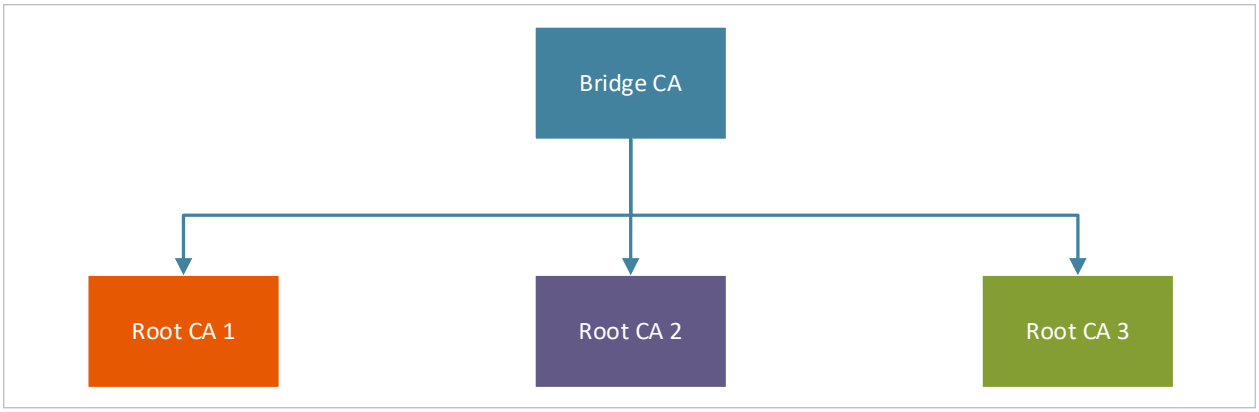


Cross-certification can also be one-way (i.e., in which Root CA 1 issues a certificate to Root CA 2, but Root CA 2 does not issue a certificate to Root CA 1). In this instance, relying parties who only trust Root CA 1 will also trust certificates issued under Root CA 2, but relying parties who only trust Root CA 2 will not trust certificates issued under Root CA 1.

The advantage of a cross-certified model is it easily allows one or more PKIs to establish mutual trust with each other. However, the model is not easily scalable as it requires each PKI operator to have a direct relationship with another and adding trust to a new PKI requires actions and agreement from all other PKIs.

Bridge CA model

The Bridge CA model builds off of the cross-certified model, with the main difference being that, rather than each Root CA cross-certifying each other, an independent Bridge CA issues one-way cross-certificates to each Root CA. Relying parties need only trust the Bridge CA and will then automatically trust any certificate from any PKI that has a cross-certificate from the Bridge CA. This allows for a more flexible hierarchy as the Bridge CA can add new PKIs without requiring any actions from existing PKIs. As the actions of the Bridge CA impact all relying parties, Bridge CAs often impose various compliance requirements (i.e., annual assurance engagements) as well as a common Certificate Policy:



What Is the Impact of Subordinate CAs?

Depending on report users' needs, Subordinate CAs may or may not be included in the scope of examination. It is important that the system description and assertion clearly articulate the hierarchy that is in scope.

What Are Some of the Business Issues Associated with CAs?

Unless they are subject to governmental licensing and regulation, CAs may use different standards or procedures to verify the identity of persons to whom they issue certificates. Thus, a digital signature is only as reliable as the CA is trustworthy in performing its functions. Consequently, a relying party needs some way to gauge how much reliance it should place on a digital signature supported by a certificate issued by a particular CA.

CA topology is a continuing issue. The most appropriate model depends on the particular business circumstances. Although it is important that public keys be certified, the issuance of nonstandard certificates can be a concern. For example, if the broadly recognised International Telecommunications Union-Telecommunication Standardization Sector's (ITU-T) X.509 data format standard is not used, subscribers and relying parties may be unable to process such certificates. Implementing the cross-certified CA model (discussed above) would also be very difficult.

Principles and Criteria for Certification Authorities

In order to be understandable to the ultimate users – the subscriber and relying party (for example, the web browser vendors) the principles set out in the following sections have been developed with the relying party in mind and, as a result, are intended to be practical and nontechnical in nature.

Certification Authorities Principles

CA business practices disclosure

The Certification Authority:

- Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement; and
- Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control policies in its Certificate Policy (if applicable).

The CA maintains effective controls to provide reasonable assurance that:

- The CA's Certification Practice Statement is consistent with its Certificate Policy (if applicable); and
- The CA provides its services in accordance with its Certificate Policy (if applicable) and Certification Practice Statement.

The Certification Authority must disclose its key and certificate life cycle management business and information privacy practices. Information regarding the CA's business practices should be made available to all subscribers and all potential relying parties, typically by posting on its Web site. Such disclosure may be contained in a Certificate Policy (CP) and/or Certification Practice Statement (CPS), or other informative materials that are available to users (subscribers and relying parties).

These WebTrust Principles and Criteria for Certification Authorities v2.2.2 recommend CAs to structure their CP and CPS documents in accordance with *IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003*. The use of I*ETF RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999* is still permitted to be used, although CAs still using RFC 2527 should transition to RFC 3647 as the use of RFC 2527 may be deprecated in future releases of these Criteria. The use of any other framework for business practice disclosures is no longer permitted in these Criteria.

Service integrity

The CA maintains effective controls to provide reasonable assurance that:

- The integrity of keys and certificates it manages is established and protected throughout their life cycles;
- The Subscriber information is properly authenticated (for the registration activities performed by ABC-CA); and
- Subordinate CA certificate and cross certificate requests are accurate, authenticated and approved.

Effective key management controls and practices are essential to the trustworthiness of the public key infrastructure. Cryptographic key management controls and practices cover CA key generation, CA key storage, backup and recovery, CA public key distribution (especially when done in the form of self-signed "root" certificates), CA key escrow (if applicable), CA key usage, CA key destruction, CA key archival, the management of CA cryptographic hardware through its life cycle, and CA-provided subscriber key management services (if applicable); and Strong key life cycle management controls are vital to guard against key compromise which can damage the integrity of the public key infrastructure.

The user certificate life cycle is at the core of the services provided by the CA. The CA establishes its standards and practices by which it will deliver services in its published CPS and Certificate Policy(s). The user certificate life cycle includes the following:

- Registration (meaning, the identification and authentication process related to binding the individual subscriber to the certificate);
- The renewal of certificates (if applicable);
- The rekey of certificates;
- The revocation of certificates;
- The suspension of certificates (if applicable);
- The timely publication of certificate status information (through Certificate Revocation Lists or some form of online certificate status protocol)
- The management of integrated circuit cards (ICCs) holding private keys through their life cycle (if applicable);
- The registration, issuance and management of subordinate CA certificates and cross-certificates.

Effective controls over the registration process are essential, as poor identification and authentication controls jeopardise the ability of subscribers and relying parties to rely on the certificates issued by the CA. Effective revocation procedures and timely publication of

certificate status information are also critical elements, as it is critical for subscribers and relying parties to know when they are unable to rely on certificates that have been issued by the CA.

CA environmental controls

The Certification Authority maintains effective controls to provide reasonable assurance that:

- Logical and physical access to CA systems and data is restricted to authorised individuals;
- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations are properly authorised and performed to maintain CA systems integrity.

The establishment and maintenance of a trustworthy CA environment is essential to the reliability of the CA's business processes. Without strong CA environmental controls, strong key and certificate life cycle management controls are severely diminished in value. CA environmental controls include CPS and CP management, security policy management, security management, asset classification and management, personnel security, physical and environmental security of the CA facility, operations management, system access management, systems development and maintenance, business continuity management, monitoring and compliance, and event journaling.

Intended Use of the WebTrust Principles and Criteria

The WebTrust Principles and Criteria for CAs can be used as a control framework to assess the adequacy of the CA systems, policies and procedures. It provides a basis for self-assessment for either development or maintaining strong PKI systems.

Assessors / practitioners can use the framework as a benchmark for performing an internal or independent assessment as an internal auditor, or an independent practitioner as supported by the CA/Browser Forum. For enrolled WebTrust practitioners, additional support is provided at www.cpacanada.ca/webtrust.

WebTrust for CA Criteria with Illustrative Controls

Illustrative controls have been included with each WebTrust criterion to provide guidance to CAs and practitioners on the types of controls that should be evaluated to achieve each criterion. These controls are not meant to be an exhaustive list, and although it is perfectly acceptable for a CA to adopt these illustrative controls in their entirety, it is recommended that CAs use these as a base and customise to their specific business processes.

1.0: CA Business Practices Disclosure[2]

The Certification Authority:

- Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practice Statement;
- Discloses its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control policies in its Certificate Policy (if applicable); and
- Provides services in accordance with its disclosed practices.

1.1 Certification Practice Statement (CPS)

The CA discloses its business practices including but not limited to the topics listed in RFC 3647 or RFC 2527 in its Certification Practice Statement.

1.2 Certificate Policy (CP) (if applicable)

The CA discloses its business practices including but not limited to the topics listed in RFC 3647 or RFC 2527 in its Certificate Policy.

Explanatory Guidance: A CA may either have separate CP and CPS documents, or a combined CP/CPS. If the CA has a combined CP/CPS, or it implements the CP defined by another CA, then Criterion 1.2 is not applicable.

2 For a public CA, such disclosure should be conducted through publication of either the Certificate Policy (CP) and/or Certification Practice Statement (CPS) on its web site. For a private CA, disclosure can be performed through alternative means, such as a corporate intranet or private web site, with access available to users (subscribers and relying parties)

2.0: CA Business Practices Management

The Certification Authority maintains effective controls to provide reasonable assurance that:

- The CA provides its services in accordance with its Certification Practice Statement and Certificate Policy (if applicable);
- The CA's Certification Practice Statement is consistent with its Certificate Policy (if applicable).

2.1 Certification Practice Statement (CPS) Management

The CA maintains controls to provide reasonable assurance that its Certification Practice Statement (CPS) management processes are effective.

ILLUSTRATIVE CONTROLS

#	Certification Practice Statement (CPS) Management
2.1.1	The PA has final authority and responsibility for approving the CA's Certification Practice Statement (CPS).
2.1.2	Responsibilities for maintaining the CPS have been formally assigned.
2.1.3	The CA's CPS is modified and approved in accordance with a defined review process.
2.1.4	The CA makes available its Certification Practice Statement (CPS) to all appropriate parties.
2.1.5	Revisions to the CA's CPS are made available to appropriate parties.
2.1.6	The CA updates its CPS to reflect changes in the environment as they occur.

2.2 Certificate Policy (CP) Management (if applicable)

The CA maintains controls to provide reasonable assurance that its Certificate Policy (CP) management process is effective.

Explanatory Guidance: A CA may either have separate CP and CPS documents, or a combined CP/CPS. If the CA has a combined CP/CPS, or it implements the CP defined by another CA, then Criterion 2.2 is not applicable.

ILLUSTRATIVE CONTROLS

#	Certificate Policy (CP) Management
2.2.1	The Policy Authority (PA) has the responsibility of defining the business requirements and policies for using digital certificates and specifying them in a Certificate Policy (CP) and supporting agreements.
2.2.2	The PA has final authority and responsibility for specifying and approving Certificate Policy(s).
2.2.3	Certificate Policy(s) are approved by the Policy Authority in accordance with a defined annual review process, including responsibilities for maintaining and tracking changes to the Certificate Policy(s).
2.2.4	A defined review process exists to assess that the Certificate Policy(s) are capable of support by the controls specified in the CPS.
2.2.5	The PA makes available the Certificate Policies supported by the CA to Subscribers and Relying Parties.

2.3 CP and CPS Consistency (if applicable)

The CA maintains controls to provide reasonable assurance that its Certification Practice Statement addresses the topics included in its Certificate Policy.

Explanatory Guidance: A CA may either have separate CP and CPS documents, or a combined CP/CPS. If the CA has a combined CP/CPS, then Criterion 2.3 is not applicable. However, if the CA implements the CP defined by another CA, then this criterion is relevant for ensuring the CA's developed CPS is consistent with the provided CP.

ILLUSTRATIVE CONTROLS

#	CP and CPS Consistency
2.3.1	The PA is responsible for ensuring that the CA's control processes, as stated in a Certification Practice Statement (CPS) or equivalent, fully comply with the requirements of the CP.
2.3.2	The CA addresses the requirements of the CP when developing its CPS.
2.3.3	The CA assesses the impact of proposed CPS changes to ensure that they are consistent with the CP.
2.3.4	A defined review process exists to ensure that Certificate Policy(s) are supported by the CA's CPS.

3.0: CA Environmental Controls

The Certification Authority maintains effective controls to provide reasonable assurance that:

- Logical and physical access to CA systems and data is restricted to authorised individuals;
- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations are properly authorised and performed to maintain CA systems integrity.

3.1 Security Management

The CA maintains controls to provide reasonable assurance that:

- security is planned, managed and supported within the organisation;
- security risks are identified and managed;
- the security of CA facilities, systems and information assets accessed by third parties is maintained; and
- the security of subscriber and relying party information is maintained when the responsibility for CA sub-functions has been outsourced to another organisation or entity.

ILLUSTRATIVE CONTROLS

Criterion	#	Security Management
Information security policy	**3.1.1**	An information security policy document, that includes physical, personnel, procedural and technical controls, is approved by management, published and communicated to all employees.
	3.1.2	Responsible management of the CA demonstrates that the information security policy is implemented and adhered to.

Criterion	#	Security Management
Information security policy *(cont'd)*	**3.1.3**	The information security policy includes the following: a. a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing; b. a statement of management intent, supporting the goals and principles of information security; c. an explanation of the security policies, principles, standards and compliance requirements of particular importance to the organisation; d. a definition of general and specific responsibilities for information security management, including reporting security incidents; and e. references to documentation, which supports the policy.
	3.1.4	There is a defined review process for maintaining the information security policy, including responsibilities and review dates.
Information security infrastructure	**3.1.5**	Senior management and/or a high-level management information security committee have the responsibility to ensure there is clear direction and management support to manage risks effectively.
	3.1.6	A management group or security committee exists to co-ordinate the implementation of information security controls and the management of risk.
	3.1.7	Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined.
	3.1.8	A management authorisation process for new information processing facilities exists and is followed.
Security of third party access	**3.1.9**	Procedures exist and are enforced to control physical and logical access to CA facilities and systems by third parties (e.g., on-site contractors, trading partners and joint ventures).
	3.1.10	If there is a business need for the CA to allow third party access to CA facilities and systems, a risk assessment is performed to determine security implications and specific control requirements.
	3.1.11	Arrangements involving third party access to CA facilities and systems are based on a formal contract containing necessary security requirements.

Criterion	#	Security Management
Outsourcing	**3.1.12**	If the CA outsources the management and control of all or some of its information systems, networks, and/or desktop environments, the security requirements of the CA are addressed in a contract agreed upon between the parties.
	3.1.13	If the CA chooses to delegate a portion of the CA roles and respective functions to another party, the CA maintains responsibility for the completion of the outsourced functions and the definition and maintenance of a statement of its CPS.

3.2 Asset Classification and Management

The CA maintains controls to provide reasonable assurance that CA assets and subscriber and relying party information receive an appropriate level of protection based upon identified risks and in accordance with the CA's disclosed business practices.

ILLUSTRATIVE CONTROLS

#	Asset Classification and Management
3.2.1	Owners are identified for all CA assets and assigned responsibility for the protection of the assets.
3.2.2	Inventories of CA assets are maintained.
3.2.3	The CA has implemented information classification and associated protective controls for information based on business needs and the business impacts associated with such needs.
3.2.4	Information labelling and handling are performed in accordance with the CA's information classification scheme and documented procedures.

3.3 Personnel Security

The CA maintains controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.

ILLUSTRATIVE CONTROLS

#	Personnel Security
3.3.1	The CA employs personnel (i.e., employees and contractors) who possess the relevant skills, knowledge and experience required for the job function.
3.3.2	Security roles and responsibilities, as specified in the organisation's security policy, are documented in job descriptions.
3.3.3	Trusted Roles, on which the security of the CA's operation is dependent, are clearly identified. Trusted roles include, at a minimum, the following responsibilities: a. overall responsibility for administering the implementation of the CA's security practices; b. approval of the generation, revocation and suspension of certificates; c. installation, configuration and maintenance of the CA systems; d. day-to-day operation of CA systems and system backup and recovery; e. viewing and maintenance of CA system archives and audit logs; f. cryptographic key life cycle management functions (e.g., key component custodians); and g. CA systems development.
3.3.4	The CA's policies and procedures specify the background checks and clearance procedures required for Trusted Roles and non-trusted roles. As a minimum, verification checks on permanent staff are performed at the time of job application and periodically for those individuals undertaking Trusted Roles.
3.3.5	An individual's trusted status is approved prior to gaining access to systems / facilities or performing actions requiring trusted status.
3.3.6	CA Employees and Trusted Roles sign a confidentiality (non-disclosure) agreement as a condition of employment.
3.3.7	Contractors who perform Trusted Roles are subject to at least the same background check and personnel management procedures as employees.

#	Personnel Security
3.3.8	Any contract arrangement between Contractors and CAs allows for the provision of temporary contract personnel that explicitly allows the organisation to take measures against contract staff who violate the organisation's security policies. Protective measures may include: a. bonding requirements on contract personnel; b. indemnification for damages due to contract personnel wilful harmful actions; and c. financial penalties.
3.3.9	Periodic reviews occur to verify the continued trustworthiness of personnel involved in the activities related to key management and certificate management.
3.3.10	A formal disciplinary process exists and is followed for employees who have violated organisational security policies and procedures. The CA's policies and procedures specify the sanctions against personnel for unauthorised actions, unauthorised use of authority, and unauthorised use of systems.
3.3.11	Physical and logical access to CA facilities and systems is disabled upon termination of employment.
3.3.12	If required based on a risk assessment, duress alarms are provided for users who might be the target of coercion.
3.3.13	All employees of the organisation and, where relevant, third party contractors, receive appropriate training in organisational policies and procedures. The CA's policies and procedures specify the following: a. The training requirements and training procedures for each role; and b. Any retraining period and retraining procedures for each role.

3.4 Physical and Environmental Security

The CA maintains controls to provide reasonable assurance that:

- physical access to CA facilities and equipment is limited to authorised individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control;
- CA facilities and equipment are protected from environmental hazards;
- loss, damage or compromise of assets and interruption to business activities are prevented; and
- compromise of information and information processing facilities is prevented.

Explanatory Guidance: 'Dual Custody Control' requires the CA to have controls in place to require at least two trusted people be present during the duration of the authorised activity in order to physically access CA systems. An example of this is an access control system requiring two people to each present their badges and second factor (i.e., biometrics, PIN) prior to access being granted to the facility.

ILLUSTRATIVE CONTROLS

Criterion	#	Physical and Environmental Security
CA facility physical security	**3.4.1**	Entry to the building or site containing the CAs certificate manufacturing facility is achieved only through a limited number of controlled access points.
	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.
	3.4.3	A manned reception area or other means to control physical access is in place to restrict access to the building or site housing CA operations to authorised personnel only.
	3.4.4	Physical barriers are in place (e.g., solid walls that extend from real floor to real ceiling) to prevent unauthorised entry and environmental contamination to the CAs certificate manufacturing facility.
	3.4.5	Physical barriers are in place (e.g., Faraday cage) to prevent electromagnetic radiation emissions for all Root CA operations (e.g., key generation and certification of CA Certificates) as disclosed in CP and/or CPS.
	3.4.6	Fire doors exist on security perimeters around CA operational facilities and are alarmed and conform to local fire regulations.
	3.4.7	Intruder detection systems are installed and regularly tested to cover all external doors of the building housing the CA operational facilities.
	3.4.8	CA operational facilities are physically locked and alarmed when unoccupied.

Criterion	#	Physical and Environmental Security
CA facility physical security *(cont'd)*	**3.4.9**	All personnel are required to wear visible identification. Employees are encouraged to challenge anyone not wearing visible identification.
	3.4.10	Access to CA operational facilities is controlled and restricted to authorised persons through the use of multi-factor authentication controls.
	3.4.11	All personnel entering and leaving CA operational facilities are logged (i.e., an audit trail of all access is securely maintained).
	3.4.12	Entry, exit, and activities within CA facilities are monitored by cameras.
	3.4.13	Visitors to CA facilities are supervised and their date and time of entry and departure recorded.
	3.4.14	Third party support services personnel is granted restricted access to secure CA operational facilities only when required and such access is authorised and accompanied.
	3.4.15	Access rights to CA facilities are regularly reviewed and updated.
Equipment security	**3.4.16**	The CA maintains an equipment inventory.
	3.4.17	Equipment is sited or protected such as to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.
	3.4.18	Equipment is protected from power failures and other electrical anomalies.
	3.4.19	Power and telecommunications, within the facility housing the CA operation, cabling carrying data or supporting CA services is protected from interception or damage.
	3.4.20	Equipment is maintained in accordance with the manufacturer's instructions and/or other documented procedures.
	3.4.21	All items of equipment containing storage media (fixed and removable disks) are checked to ensure that they do not contain sensitive data prior to their disposal. Storage media containing sensitive data is physically destroyed or securely overwritten prior to disposal or reused.

Criterion	#	Physical and Environmental Security
General controls	**3.4.22**	Sensitive or critical business information is locked away when not required and when the CA facility is vacated.
	3.4.23	Procedures require that personal computers and workstations are logged off or protected by key locks, passwords or other controls when not in use.
	3.4.24	The movement of materials to/from the CA facility requires prior authorisation.

3.5 Operations Management

The CA maintains controls to provide reasonable assurance that:

- the secure operation of CA information processing facilities is ensured;
- the risk of CA systems failure is minimised;
- the integrity of CA systems and information is protected against viruses and malicious software;
- damage from security incidents and malfunctions is minimised through the use of incident reporting and response procedures; and
- media are securely handled to protect them from damage, theft and unauthorised access.

ILLUSTRATIVE CONTROLS

Criterion	#	Operations Management
Operational procedures and responsibilities	**3.5.1**	CA operating procedures are documented and maintained for each functional area.
	3.5.2	Formal management responsibilities and procedures exist to control all changes to CA equipment, software and operating procedures.
	3.5.3	Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorised modification or misuse of information or services.
	3.5.4	Development and testing facilities are separated from operational facilities.
	3.5.5	Prior to using external facilities management services, risks and related controls are identified, agreed upon with the contractor, and incorporated into the contract.

Criterion	#	Operations Management
System planning and acceptance	**3.5.6**	Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.
	3.5.7	Acceptance criteria for new information systems, upgrades and new versions are established and suitable tests of the system carried out prior to acceptance.
Protection against viruses and malicious software	**3.5.8**	Detection and prevention controls to protect against viruses and malicious software, including on offline or air gapped systems are implemented. Employee awareness programs are in place.
Incident reporting and response	**3.5.9**	A formal security incident reporting procedure exists setting out the actions to be taken on receipt of an incident report. This includes a definition and documentation of assigned responsibilities and escalation procedures. Any incidents are reported to responsible management as a matter of urgency.
	3.5.10	Users of CA systems are required to note and report observed or suspected security weaknesses in, or threats to, systems or services as they are detected.
	3.5.11	Procedures exist and are followed for reporting hardware and software malfunctions.
	3.5.12	Procedures exist and are followed to assess that corrective action is taken for reported incidents.
	3.5.13	A formal problem management process exists that allows the types, volumes and impacts of incidents and malfunctions to be documented, quantified and monitored.
Media handling and security	**3.5.14**	Procedures for the management of removable computer media require the following: a. if no longer required, the previous contents of any reusable media that are to be removed from the organisation are erased or media is destroyed; b. authorisation is required for all media removed from the organisation and a record of all such removals to maintain an audit trail is kept; and c. all media are stored in a safe, secure environment, in accordance with manufacturers' specifications.

Criterion	#	Operations Management
Media handling and security *(cont'd)*	**3.5.15**	Equipment containing storage media (i.e., fixed hard disks) is checked to determine whether they contain any sensitive data prior to disposal or reuse. Storage devices containing sensitive information are physically destroyed or securely overwritten prior to disposal or reuse.
	3.5.16	Procedures for the handling and storage of information exist and are followed in order to protect such information from unauthorised disclosure or misuse.
	3.5.17	System documentation is protected from unauthorised access.

3.6 System Access Management

The CA maintains controls to provide reasonable assurance that CA system access is limited to authorised individuals. Such controls provide reasonable assurance that:

- hypervisor, operating system, database, and network device access is limited to authorised individuals with predetermined task privileges;
- access to network segments housing CA systems is limited to authorised individuals, applications and services; and
- CA application use is limited to authorised individuals.

ILLUSTRATIVE CONTROLS

Criterion	#	System Access Management
User access management	**3.6.1**	Business requirements for access control are defined and documented in an access control policy that includes at least the following: a. roles and corresponding access permissions; b. identification and authentication process for each user; c. segregation of duties; and d. number of persons required to perform specific CA operations (i.e., m of n rule where m represents the number of key shareholders required to perform an operation and n represents the total number of key shares).
	3.6.2	There is a formal user registration and de-registration procedure for access to CA information systems and services, including hypervisors, operating systems, database, and network devices.

Criterion	#	System Access Management
User access management *(cont'd)*	**3.6.3**	The allocation and use of privileges is restricted and controlled.
	3.6.4	The allocation of passwords and multi-factor authentication tokens is controlled through a formal management process.
	3.6.5	Access rights for users with trusted roles are reviewed at regular intervals and updated.
	3.6.6	Users are required to follow defined policies and procedures in the selection and use of passwords.
	3.6.7	Users are required to ensure that unattended equipment has appropriate protection.
	3.6.8	Where technically feasible, administrative and superuser accounts require the use of multi-factor authentication controls.
Network access control	**3.6.9**	CA employed personnel are provided direct access only to the services that they have been specifically authorised to use. The path from the user terminal to computer services is controlled.
	3.6.10	Remote access to CA systems, made by CA employees or external systems, if permitted, requires authentication.
	3.6.11	Connections made by CA employees or CA systems to remote computer systems are authenticated.
	3.6.12	Access to diagnostic ports is securely controlled.
	3.6.13	Controls (e.g., firewalls) are in place to protect the CA's internal network domain from any unauthorised access from any other domain.
	3.6.14	Controls are in place to limit the network services (e.g., HTTP, FTP, etc.) available to authorised users in accordance with the CA's access control policies. The security attributes of all network services used by the CA organisation are documented by the CA.
	3.6.15	Routing controls are in place to ensure that computer connections and information flows do not breach the CA's access control policy.

Criterion	#	System Access Management
Network access control *(cont'd)*	**3.6.16**	The CA maintains local network components (e.g., firewalls and routers) in a physically secure environment and audits their configurations periodically for compliance with the CA's configuration requirements.
	3.6.17	Sensitive data is encrypted when exchanged over public or untrusted networks.
Hypervisor, operating system, database, and network device access control	**3.6.18**	Hypervisors, operating systems, databases, and network devices are configured in accordance with the CA's system configuration standards and periodically reviewed and updated.
	3.6.19	Hypervisors, operating system, database, and network device patches and updates are applied in a timely manner when deemed necessary based on a risk assessment and follow formal change management procedures (see § 3.7).
	3.6.20	Automatic terminal identification is used to authenticate connections to specific locations and to portable equipment.
	3.6.21	Access to CA systems requires a secure logon process.
	3.6.22	All CA personnel users have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual. Where shared or group accounts are required, other monitoring controls are implemented to maintain individual accountability.
	3.6.23	Uses of system utility programs are restricted to authorised personnel and tightly controlled.
	3.6.24	Inactive terminals serving CA systems require re-authentication prior to use.
	3.6.25	Restrictions on connection times are used to provide additional security for high-risk applications.
	3.6.26	Sensitive data is protected against disclosure to unauthorised users.

Criterion	#	System Access Management
Application access control	**3.6.27**	Access to information and application system functions is restricted in accordance with the CA's access control policy.
	3.6.28	CA personnel are successfully identified and authenticated before using critical applications related to certificate management.
	3.6.29	Sensitive systems (e.g., Root CA) require a dedicated (isolated) computing environment.

3.7 Systems Development, Maintenance, and Change Management

The CA maintains controls to provide reasonable assurance that CA systems development, maintenance activities, patching, and changes to CA systems including hypervisors (where applicable), operating systems, databases, applications, network devices, and hardware are documented, tested, authorised, and properly implemented to maintain CA system integrity.

ILLUSTRATIVE CONTROLS

#	Systems Development, Maintenance, and Change Management
3.7.1	Business requirements for new systems, or enhancements to existing systems specify the control requirements.
3.7.2	Software testing and change control procedures exist and are followed for the implementation of software on operational systems including scheduled software releases, modifications, patches, and emergency software fixes.
3.7.3	Change control procedures exist and are followed for the hardware, network component, and system configuration changes.
3.7.4	Test data is protected and controlled.
3.7.5	Control is maintained over access to program source libraries.
3.7.6	Application systems are reviewed and tested when operating system changes occur.
3.7.7	The implementation of changes is strictly controlled by the use of formal change control procedures to minimise the risk of corruption of information systems.
3.7.8	Modifications to software packages are discouraged and all changes are strictly controlled.

#	Systems Development, Maintenance, and Change Management
3.7.9	The purchase, use and modification of software are controlled and checked to protect against possible covert channels and Trojan code. This includes the authentication of the source of the software. These controls apply equally to outsourced software development.

3.8 Disaster Recovery, Backups, and Business Continuity Management

The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster or other type of business interruption. Such controls include, at a minimum:

- the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system;
- the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
- creating backups of systems, data, and configuration information at regular intervals in accordance with the CA's disclosed business practices, and storage of these backups at an alternate location; and
- the availability of an alternate site, equipment and connectivity to enable recovery.

The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation or degradation of the CA's services.

ILLUSTRATIVE CONTROLS

#	Disaster Recovery, Backups, and Business Continuity Management
3.8.1	The CA has a managed process for developing and maintaining its business continuity plans. The CA has a business continuity planning strategy based on an appropriate risk assessment.

#	Disaster Recovery, Backups, and Business Continuity Management
3.8.2	The CA has a business continuity plan to maintain or restore the CA's operations in a timely manner following interruption to, or failure of, critical CA processes. The CA's business continuity plan addresses the following: a. the conditions for activating the plans; b. emergency procedures; c. fall-back procedures; d. resumption procedures; e. a maintenance schedule for the plan; f. awareness and education requirements; g. the responsibilities of the individuals; h. recovery time objective (RTO) and recovery point objective (RPO); and i. regular testing of contingency plans.
3.8.3	The CA's business continuity plans include disaster recovery processes for all critical components of a CA system, including the hardware, software and keys, in the event of a failure of one or more of these components. Specifically: a. cryptographic devices used for storage of backup CA private keys are securely stored at an off-site location in order for the CA to recover in the event of a disaster at the primary CA facility; and b. the requisite secret key shares or key components, needed to use and manage the disaster recovery cryptographic devices, are securely stored at an off-site location.
3.8.4	Backup copies of essential business information are regularly taken. The security requirements of these copies are consistent with the controls for the information backed up.
3.8.5	The CA identifies and arranges for an alternate site where core PKI operations can be restored in the event of a disaster at the CA's primary site. Fall-back equipment and backup media are sited at a safe distance to avoid damage from disaster at the main site.
3.8.6	The CA's business continuity plans include procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.
3.8.7	The CA's business continuity plans address the recovery procedures used when computing resources, software, and/or data are corrupted or suspected to be corrupted.
3.8.8	Business continuity plans are tested regularly to ensure that they are up to date and effective.

#	Disaster Recovery, Backups, and Business Continuity Management
3.8.9	Business continuity plans define an acceptable system outage time, recovery time, and the average time between failures as disclosed in the CP and/or CPS.
3.8.10	Business continuity plans are maintained by regular reviews and updates to ensure their continuing effectiveness.
3.8.11	The CA maintains procedures for the termination, notification of affected entities, and for transferring relevant archived CA records to a custodian as disclosed in the CP and/or CPS.

3.9 Monitoring and Compliance

The CA maintains controls to provide reasonable assurance that:

- it conforms with the relevant legal, regulatory and contractual requirements;
- compliance with the CA's security policies and procedures is ensured;
- the effectiveness of the system audit process is maximised and interference to and from the system audit process is minimised; and
- unauthorised CA system usage is detected.

Explanatory Guidance: This Criterion addresses the existence of controls and business processes the CA has in place to help ensure it complies with all relevant legal requirements. An example would be testing if a framework is in place to help track requirements and monitor compliance. However, a practitioner would not test if the CA is actually in compliance with its legal requirements, and no assurance over the CA's compliance status can be provided.

ILLUSTRATIVE CONTROLS

Criterion	#	Monitoring and Compliance
Compliance with legal requirements	**3.9.1**	Relevant statutory, regulatory and contractual requirements are explicitly defined and documented.
	3.9.2	The CA has implemented procedures to comply with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.

Criterion	#	Monitoring and Compliance
Compliance with legal requirements *(cont'd)*	**3.9.3**	Controls are in place to ensure compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic hardware and software.
	3.9.4	Procedures exist to ensure that personal information is protected in accordance with relevant legislation.
	3.9.5	The information security policy addresses the following: a. the information that must be kept confidential by CA or RA; b. the information that is not considered confidential; c. the policy on release of information to law enforcement officials; d. information that can be revealed as part of civil discovery; e. the conditions upon which information may be disclosed with the subscriber's consent; and f. any other circumstances under which confidential information may be disclosed.
	3.9.6	CA records are protected from loss, unauthorised destruction and falsification.
	3.9.7	Management authorises the use of information processing facilities and controls are applied to prevent the misuse of such facilities.
Review of security policy and technical compliance	**3.9.8**	Managers are responsible for ensuring that security procedures within their area of responsibility are carried out correctly.
	3.9.9	The CA's operations are subject to regular review to ensure timely compliance with its CPS.
	3.9.10	CA systems are periodically checked for compliance with security implementation standards.
System audit process	**3.9.11**	Audits of operational systems are planned and agreed such as to minimise the risk of disruptions to business processes.
	3.9.12	Access to system audit tools is protected to prevent possible misuse or compromise.
Monitoring system access and use	**3.9.13**	Procedures for monitoring the use of CA systems are established which include the timely identification and follow up of unauthorised or suspicious activity. Alerting mechanisms are implemented to detect unauthorised access.

3.10 Audit Logging

The CA maintains controls to provide reasonable assurance that:

- significant CA environmental, key management, and certificate management events are accurately and appropriately logged;
- the confidentiality and integrity of current and archived audit logs are maintained;
- audit logs are completely and confidentially archived in accordance with disclosed business practices; and
- audit logs are reviewed periodically by authorised personnel.

ILLUSTRATIVE CONTROLS

Criterion	#	Audit Logging
Audit logs	**3.10.1**	The CA generates automatic (electronic) and manual audit logs in accordance with the requirements of the CP and/or CPS.
	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.

Criterion	#	Audit Logging
Events logged	**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.
	3.10.4	The CA logs the following cryptographic device life cycle management related events: a. device receipt and installation; b. placing into or removing a device from storage; c. device activation and usage; d. device de-installation; e. designation of a device for service and repair; and f. device retirement.

Criterion	#	Audit Logging
Events logged *(cont'd)*	**3.10.5**	If the CA provides subscriber key management services, the CA logs the following subscriber key life cycle management related events: a. key generation; b. key distribution (if applicable); c. key backup (if applicable); d. key escrow (if applicable); e. key storage; f. key recovery (if applicable); g. key archival (if applicable); h. key destruction; i. identity of the entity authorising a key management operation; and j. key compromise.
	3.10.6	The CA records (or requires that the RA record) the following certificate application information: a. the method of identification applied and information used to meet subscriber requirements; b. record of unique identification data, numbers, or a combination thereof (e.g., applicants drivers license number) of identification documents, if applicable; c. storage location of copies of applications and identification documents; d. identity of entity accepting the application; e. method used to validate identification documents, if any; f. name of receiving CA or submitting RA, if applicable; g. the subscriber's acceptance of the Subscriber Agreement; and h. where required under privacy legislation, the Subscriber's consent to allow the CA to keep records containing personal data, pass this information to specified third parties, and publication of certificates.

Criterion	#	Audit Logging
Events logged *(cont'd)*	**3.10.7**	The CA logs the following certificate life cycle management related events: a. receipt of requests for certificate(s) – including initial certificate requests, renewal requests and rekey requests; b. submissions of public keys for certification; c. change of affiliation of an entity; d. generation of certificates; e. distribution of the CA's public key; f. certificate revocation requests; g. certificate revocation; h. certificate suspension requests (if applicable); i. certificate suspension and reactivation; and j. generation and issuance of Certificate Revocation Lists.
	3.10.8	The CA logs the following security-sensitive events: a. security-sensitive files or records read or written including the audit log itself; b. actions taken against security-sensitive data; c. security profile changes; d. use of identification and authentication mechanisms, both successful and unsuccessful (including multiple failed authentication attempts); e. system crashes, hardware failures and other anomalies; f. actions taken by individuals in Trusted Roles, computer operators, system administrators, and system security officers; g. change of affiliation of an entity; h. decisions to bypass encryption/authentication processes or procedures; and i. access to the CA system or any component thereof.
	3.10.9	Audit logs do not record the private keys in any form (e.g., plaintext or enciphered).
	3.10.10	CA computer system clocks are synchronised for accurate recording as defined in the CP and/or CPS that specifies the accepted time source.

Criterion	#	Audit Logging
Audit log protection	**3.10.11**	Current and archived audit logs are maintained in a form that prevents their modification, substitution, or unauthorised destruction.
	3.10.12	Digital signatures are used to protect the integrity of audit logs where applicable or required to satisfy legal requirements.
	3.10.13	The private key used for signing audit logs is not used for any other purpose. This applies equally to a symmetric secret key used with a symmetric MAC mechanism.
Audit log archival	**3.10.14**	The CA archives audit log data on a periodic basis as disclosed in the CP and/or CPS.
	3.10.15	In addition to possible regulatory stipulation, a risk assessment is performed to determine the appropriate length of time for retention of archived audit logs.
	3.10.16	The CA maintains archived audit logs at a secure off-site location for a predetermined period as determined by risk assessment and legal requirements.
Review of audit logs	**3.10.17**	Current and archived audit logs are only retrieved by authorised individuals for valid business or security reasons.
	3.10.18	Audit logs are reviewed periodically according to the practices established in the CPS. The review of current and archived audit logs include a validation of the audit logs' integrity, and the timely identification and follow up of unauthorised or suspicious activity.

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.

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

Criterion	#	CA Key Generation
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 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).
	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.
	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.
	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.

Criterion	#	CA Key Generation
Generation of CA keys including root CA keys – script requirements	**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).
	4.1.7	The integrity of the hardware/software used for key generation and the interfaces to the hardware/software is tested before production usage.

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

#	CA Key Storage, Backup, and Recovery
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.

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

#	CA Public Key Distribution
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.

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

#	CA Key Usage
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.

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.

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.

#	CA Key Destruction
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; • HSM and/or cryptographic hardware zeroisation/initialisation • HSM and/or cryptographic hardware physical destruction • 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.

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

#	CA Key Compromise
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.
4.7.6	The CA's business continuity plan considers key replication techniques.

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

#	CA Cryptographic Hardware Life Cycle Management
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).

#	CA Cryptographic Hardware Life Cycle Management
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.

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 4.9 is not applicable.

ILLUSTRATIVE CONTROLS

#	CA Key Escrow
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.

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

#	CA Key Transportation
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.

#	CA Key Transportation
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.

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 4.11.

ILLUSTRATIVE CONTROLS

#	CA Key Migration
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).
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).

#	CA Key Migration
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).

5.0: Subscriber Key Lifecycle Controls

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

5.1 CA-Provided Subscriber Key Generation Services (if supported)

The CA maintains controls to provide reasonable assurance that:

- subscriber keys generated by the CA (or RA or card bureau) are generated within a secure cryptographic device based on a risk assessment and the business requirements of the CA in accordance with the CA's disclosed business practices; and
- subscriber keys generated by the CA (or RA or card bureau) are securely distributed to the subscriber by the CA (or RA or card bureau) in accordance with the CA's disclosed business practices.

Explanatory Guidance: CA-Provided Subscriber Key Generation refers to the practice of the CA securely generating the public-private key pair to be used by a subscriber, and then securely delivering this key pair along with the certificate to the subscriber. Sometimes, a CA may do this for certain types of certificates (i.e., S/MIME) but not for others (i.e., SSL/TLS).

This Criterion 5.1 is only applicable if the CA is performing this generation and delivery itself. In some instances, the subscriber may access a CA-hosted webpage which utilises the subscriber's local crypto-toolkit to automate the key generation and certificate request process in the background. Although this may appear as if the CA is generating the subscriber's key pair, it is in fact not and this Criterion would not be applicable.

ILLUSTRATIVE CONTROLS

Criterion	#	CA-Provided Subscriber Key Generation Services
CA (or RA or Card Bureau) provided subscriber key generation	**5.1.1**	Subscriber key generation is performed within a secure cryptographic device meeting the applicable ISO 15782-1/FIPS 140-2/ANSI x9.66 requirements based on a risk assessment and the business requirements of the CA and in accordance with the applicable CP. Such cryptographic devices perform subscriber key generation using a random number generator (RNG) or pseudo random number generator (PRNG) as specified in the ANSI X9 or ISO standard ISO/IEC 18032.
	5.1.2	Subscriber key generation performed by the CA (or RA or card bureau) uses a key generation algorithm as specified in the CP.
	5.1.3	Subscriber key generation performed by the CA (or RA) uses a prime number generator as specified in an ANSI X9 or ISO standard.
	5.1.4	Subscriber key generation performed by the CA (or RA or card bureau) results in key sizes in accordance with the CP.
	5.1.5	Subscriber key generation performed by the CA (or RA) is performed by authorised personnel in accordance with the CA's CPS.
	5.1.6	When subscriber key generation is performed by the CA (or RA or card bureau), the CA (or RA or card bureau) securely (confidentially) delivers the subscriber key pair(s) generated by the CA (or RA or card bureau) to the subscriber in accordance with the CP.

5.2 CA-Provided Subscriber Key Storage and Recovery Services (if supported)

The CA maintains controls to provide reasonable assurance that:

- subscriber private keys stored by the CA remain confidential and maintain their integrity;
- subscriber private keys archived and escrowed by the CA remain confidential; and
- subscriber private keys stored by the CA are completely destroyed at the end of the key pair life cycle.

Explanatory Guidance: CA-Provided Subscriber Key Storage and Recovery Services refers to the practice of the CA maintaining a copy of the subscriber's **private** key for backup, archive, and/or escrow purposes. (The CA already maintains a copy of the **public** key as part of the certificate). If the CA generates the subscriber's key pair (see §5.1), this this Criterion 5.2 would also be applicable as the CA will have to store the subscriber's key pair until it is delivered to the subscriber.

ILLUSTRATIVE CONTROLS

Criterion	#	CA-Provided Subscriber Key Storage and Recovery Services
CA-provided subscriber key storage, backup and recovery	**5.2.1**	Subscriber private keys stored by the CA (or RA) are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and requirements of the CP.
	5.2.2	If the CA generates key pair(s) on behalf of a Subscriber, the CA (or RA) ensures that the subscriber's private keys are not disclosed to any entity other than the owner (i.e., the subscriber) of the keys.
	5.2.3	If the CA (or RA) generates public/private signing key pair(s), it does not maintain a copy of any private signing key, once the subscriber confirms receipt of that key.
	5.2.4	If the CA (or RA) provides subscriber (confidentiality) key storage, backup and recovery, subscriber private (confidentiality) key backup and recovery services are only performed by authorised personnel.
	5.2.5	If the CA (or RA) provides subscriber key storage, backup and recovery, controls exist to ensure that the integrity of the subscriber's private (confidentiality) key is maintained throughout its life cycle.
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.
	5.2.7	If the CA provides subscriber (confidentiality) key archival, all archived Subscriber keys are destroyed at the end of the archive period.

Criterion	#	CA-Provided Subscriber Key Storage and Recovery Services
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.
	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.

5.3 Integrated Circuit Card (ICC) Lifecycle Management (if supported)

The CA maintains controls to provide reasonable assurance that:

- ICC procurement, preparation and personalisation are securely controlled by the CA (or RA or card bureau);
- ICC Application Data File (ADF) preparation is securely controlled by the CA (or RA);
- ICC usage is enabled by the CA (or RA or card bureau) prior to ICC issuance;
- ICC deactivation and reactivation are securely controlled by the CA (or RA);
- ICCs are securely stored and distributed by the CA (or RA or card bureau);
- ICCs are securely replaced by the CA (or RA or card bureau); and
- ICCs returned to the CA (or RA or card bureau) are securely terminated.

Explanatory Guidance: Integrated Circuit Card (ICC)s refer to any secure smartcard-like device that will be used for the storage of sensitive data and processing of cryptographic devices. ICCs may take on different form factors including the traditional ISO/IEC 7810 card, USB tokens, key fobs, wearables, and embedded secure elements in computing and mobile devices. ICCs can operate through a 'contact' interface (i.e., by inserting a card into a reader, plugging in a USB token to a computer, etc.), and through a 'contactless' interface (i.e., by tapping or waving a card or device on or near a reader). Some ICCs may have both 'contact' and 'contactless' interfaces (e.g., EMV bankcards in many countries).

In some cases, a CA may be involved in the entire ICC lifecycle, including procurement, personalisation, distribution, and replacement/destruction. In other cases, the CA's involvement may be limited to certifying a key pair generated by the subscriber on their own ICC (e.g., as part of the provisioning process for payment credentials of a mobile wallet, the CA may certify the key pair generated in the secure element of the subscriber's mobile device).

ILLUSTRATIVE CONTROLS

Criterion	#	Integrated Circuit Card (ICC) Lifecycle Management
ICC procurement	**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.
	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.
	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.

Criterion	#	Integrated Circuit Card (ICC) Lifecycle Management
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).
	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.

Criterion	#	Integrated Circuit Card (ICC) Lifecycle Management
ICC storage and distribution	**5.3.13**	ICCs are securely stored prior to distribution.
	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.
	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).
	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.
	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.
	5.3.21	The ICC is used by the subscriber or where applicable the Subscriber in accordance within the terms of the CP.

Criterion	#	Integrated Circuit Card (ICC) Lifecycle Management
ICC deactivation and reactivation	**5.3.22**	Application Data File (ADF) deactivation can be performed only by the CA, as the application supplier.
	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.
	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.
	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.

5.4 Requirements for Subscriber Key Management

The CA maintains controls to provide reasonable assurance that:

- requirements for protection of subscriber keys are communicated to subscribers; and
- any subscriber key management tools provided by the CA support the requirements of the CA's business practices disclosure.

ILLUSTRATIVE CONTROLS

Criterion	#	Requirements for Subscriber Key Management
Subscriber key generation	**5.4.1**	The CP specifies the appropriate ISO 19790/FIPS 140-2 level requirement for cryptographic modules used for subscriber key generation.
	5.4.2	The CP specifies the key generation algorithm(s) that is used for subscriber key generation.
	5.4.3	The CP specifies the acceptable key sizes for subscriber key generation.
Subscriber key storage, backup and recovery	**5.4.4**	The CA or RA provides or makes available the mechanisms to allow the Subscriber to access (i.e., private key owner verification method), manage and control the usage of their private keys.
	5.4.5	The CP specifies the private key protection requirements for stored subscriber private keys.
	5.4.6	The CP states the circumstances and authority of when the subscriber's private key will be restored and the control processes.
	5.4.7	The CP specifies the private key protection requirements for backup copies of subscriber private keys stored by the subscriber.
Subscriber key usage	**5.4.8**	Subscriber Agreements describe the required processes to be followed by the Subscriber of any use of the cryptographic mechanism (e.g., HSM or ICC and software application).
	5.4.9	The CP specifies the acceptable uses for subscriber key pairs.
	5.4.10	The CP specifies the requirements for subscriber key usage.
Subscriber key archival	**5.4.11**	The CP specifies the private key protection requirements for archived subscriber private keys.
	5.4.12	The CP specifies the requirements for destruction of archived subscriber keys at the end of the archive period.

Criterion	#	Requirements for Subscriber Key Management
Subscriber key destruction	**5.4.13**	The CP specifies the means through which subscriber key destruction is performed.
	5.4.14	The CP or CPS specifies the requirements for destruction of all copies and fragments of the subscriber's private key at the end of the key pair life cycle.
Subscriber cryptographic hardware life cycle management	**5.4.15**	If required, the CP specifies the requirements for use and handling of cryptographic hardware and subscriber authentication processes (and subsequent actions) where the cryptographic hardware is in other physical locations (i.e., an HSM attached to a mainframe or remote server).
Subscriber key compromise	**5.4.16**	The CP specifies the requirements for notification of the CA or RA in the event of subscriber key compromise.

6.0: Certificate Lifecycle Management

The Certification Authority maintains effective controls to provide reasonable assurance that Subscriber information was properly authenticated (for the registration activities performed by ABC-CA).

6.1 Subscriber Registration

The CA maintains controls to provide reasonable assurance that:

For authenticated certificates

- subscribers are accurately identified in accordance with the CA's disclosed business practices;
- subscribers' domain names and IP addresses are accurately validated in accordance with the CA's disclosed business practices; and
- subscribers' certificate requests are accurate, authorised and complete.

For domain validated certificates

- subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices; and
- subscriber's certificate requests are accurate and complete.

ILLUSTRATIVE CONTROLS

Criterion	#	Subscriber Registration
Identification and authentication	**6.1.1**	For authenticated certificates, the CA verifies or requires that the RA verify the credentials presented by a subscriber as evidence of identity or authority to perform a specific role in accordance with the requirements of the CP. a. For individual end entity certificates, the CA or RA verifies the identity of the person whose name is to be included in the subscriber distinguished name field of the certificate. An unauthenticated individual name is not included in the subscriber distinguished name. b. For organisational certificates (including role based, server, network resource, code signing, etc.), the CA or RA verifies the legal existence of the organisation's name and the authority of the requesting party to be included in the organisation attribute in the subscriber distinguished name field of the certificate. An unauthenticated organisation name is not included in a certificate. c. For organisational certificates containing a domain name of an organisation, the CA or RA verifies the organisation's ownership, control, or right to use the domain name and the authority of the requesting party included in the common name attribute of the subscriber distinguished name field of the certificate. An unauthenticated domain name is not included in a certificate.
	6.1.2	For domain and/or IP address validated certificates, the CA validates or requires that the RA validate (as determined by the CP) the organisation's ownership, control, or right to use the domain name and/or IP address.
	6.1.3	The CA or RA verifies the accuracy of the information included in the requesting entity's certificate request in accordance with the CP.
	6.1.4	The CA or RA checks the Certificate Request for errors or omissions in accordance with the CP.
	6.1.5	For end entity certificates, the CA uses the RA's public key contained in the requesting entity's Certificate Request to verify signature on the Certificate Request submission.
	6.1.6	The CA verifies the uniqueness of the subscriber's distinguished name within the boundaries or community defined by the CP.

Criterion	#	Subscriber Registration
Identification and authentication *(cont'd)*	**6.1.7**	Encryption and access controls are used to protect the confidentiality and integrity of registration data in transit and in storage.
	6.1.8	At the point of registration (before certificate issuance) the RA or CA informs the Subscriber of the terms and conditions regarding use of the certificate.
	6.1.9	Before certificate issuance, the CA informs the Subscriber of the terms and conditions regarding use of the certificate.
Certificate request	**6.1.10**	The CA requires that an entity requesting a certificate must prepare and submit the appropriate certificate request data (Registration Request) to an RA (or the CA) as specified in the CP.
	6.1.11	The CA requires that the requesting entity submit its public key in a self-signed message to the CA for certification. The CA requires that the requesting entity digitally sign the Registration Request using the private key that relates to the public key contained in the Registration Request in order to: a. allow the detection of errors in the certificate application process; and b. prove possession of the companion private key for the public key being registered.
	6.1.12	The certificate request is treated as acceptance of the terms of conditions by the requesting entity to use that certificate as described in the Subscriber Agreement.
	6.1.13	The CA validates the identity of the RA authorised to issue registration requests under a specific CP.
	6.1.14	The CA requires that RAs submit the requesting entity's certificate request data to the CA in a message (Certificate Request) signed by the RA. The CA verifies the RA's signature on the Certificate Request.
	6.1.15	The CA requires that the RA secure that part of the certificate application process for which it (the RA) assumes responsibility in accordance with the CA's CPS.
	6.1.16	The CA requires that RAs record their actions in an audit log.
	6.1.17	The CA verifies the authenticity of the submission by the RA in accordance with the CA's CPS.

6.2 Certificate Renewal (if supported)

The CA maintains controls to provide reasonable assurance that certificate renewal requests are accurate, authorised and complete.

Explanatory Guidance: Certificate Renewal is the process in which a subscriber can obtain a new certificate to replace an old certificate that:

- Contains the same information (identity, domains, etc.) as the old certificate
- Has a new validity period ending after the validity period of the old certificate
- Contains the **same** public key as the old certificate

If CA does not have controls in place to prevent a subscriber from using the same key pair to request a certificate that has the same information as a previously-issued and valid certificate, then it de facto supports Certificate Renewal, even if not explicitly stated.

ILLUSTRATIVE CONTROLS

Criterion	#	Certificate Renewal
Certificate renewal request	**6.2.1**	The Certificate Renewal Request includes at least the subscriber's Distinguished Name, the Serial Number of the certificate (or other information that identifies the certificate), and the requested validity period. (The CA will only renew certificates that were issued by itself.)
	6.2.2	The CA requires that the requesting entity digitally sign the Certificate Renewal Request using the private key that relates to the public key contained in the requesting entity's existing public key certificate.
	6.2.3	The CA issues a new certificate using the subscriber's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's intended lifetime and no indications exist that the subscriber's private key has been compromised.
	6.2.4	For renewal of authenticated certificates, the CA or the RA process the certificate renewal data to verify the identity of the requesting entity and to identify the certificate to be renewed.
	6.2.5	For domain validated certificates, the CA or the RA process the certificate renewal data to re-validate the domain in accordance with the requirements of the CP.
	6.2.6	The CA or the RA validate the signature on the Certificate Renewal Request.

Criterion	#	Certificate Renewal
Certificate renewal request *(cont'd)*	**6.2.7**	The CA verifies the existence and validity of the certificate to be renewed. The CA does not renew certificates that have been revoked, expired or suspended.
	6.2.8	The CA or the RA verifies that the request, including the extension of the validity period, meets the requirements defined in the CP.
	6.2.9	The CA requires that RAs submit the Certificate Renewal Data to the CA in a message (Certificate Renewal Request) signed by the RA.
	6.2.10	The CA requires that the RA secures that part of the certificate renewal process for which it (the RA) assumes responsibility in accordance with the CP.
	6.2.11	The CA requires that RAs record their actions in an audit log.
	6.2.12	The CA verifies the authenticity of the submission by the RA.
	6.2.13	The CA verifies the RA's signature on the Certificate Renewal Request.
	6.2.14	The CA checks the Certificate Renewal Request for errors or omissions. This function may be delegated explicitly to the RA.
	6.2.15	The CA or RA notifies Subscribers prior to the expiration of their certificate of the need for renewal in accordance with the CP.
	6.2.16	The CA issues a signed notification indicating the certificate renewal has been successful.
	6.2.17	The CA makes the new certificate available to the end entity in accordance with the CP.

6.3 Certificate Rekey

The CA maintains controls to provide reasonable assurance that certificate rekey requests, including requests following certificate revocation or expiration, are accurate, authorised and complete.

Explanatory Guidance: Certificate Rekey is the process in which a subscriber can obtain a new certificate to replace an old certificate that:

- Contains the same information (identity, domains, etc.) as the old certificate
- Has the same expiry date (notAfter date) as the old certificate
- Contains a different public key as the old certificate

In some cases, a CA may refer to Certificate Rekey as a 'renewal', however, if the process results in the subscriber having a new certificate issued with a different public key (whether voluntary on the part of the subscriber or mandated by the CA), then this is a Certificate Rekey. A Certificate Renewal only occurs when the same key pair is recertified (see §6.2)

ILLUSTRATIVE CONTROLS

#	Certificate Rekey
6.3.1	A Certificate Rekey Request includes at least the subscriber's distinguished name, the serial number of the certificate, and the requested validity period to allow the CA or the RA to identify the certificate to rekey.
6.3.2	The CA requires that the requesting entity digitally sign, using the existing private key, the Certificate Rekey Request containing the new public key.
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.
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.

#	Certificate Rekey
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.

6.4 Certificate Issuance

The CA maintains controls to provide reasonable assurance that certificates are generated and issued in accordance with the CA's disclosed business practices.

ILLUSTRATIVE CONTROLS

#	Certificate Issuance
6.4.1	The CA generates certificates using Certificate Request Data and manufactures the certificate as defined by the appropriate Certificate Profile in accordance with ISO 9594/X.509 and ISO 15782-1 formatting rules as disclosed within the CP.
6.4.2	Validity periods are set in the CP and are formatted in accordance with ISO 9594/X.509 and ISO 15782-1 as disclosed within the CP.
6.4.3	Extension fields are formatted in accordance with ISO 9594/X.509 and ISO 15782-1 as disclosed within the CP.
6.4.4	The CA signs the end entity's public key and other relevant information with the CA's private signing key.

#	Certificate Issuance
6.4.5	The CA publishes the certificate after the certificate has been accepted by the requesting entity as disclosed in the CA's business practices.
6.4.6	When an RA is used, the CA notifies the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request.
6.4.7	Certificates are issued based on approved subscriber registration, certificate renewal or certificate rekey requests in accordance with the CP.
6.4.8	The CA issues a signed notification to the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request.
6.4.9	The CA issues an out-of-band notification to the Subscriber when a certificate is issued. Where this notification includes initial activation data, then control processes ensure safe delivery to the Subscriber.
6.4.10	Whether certificates expire, are revoked or are suspended, copies of certificates are retained for the appropriate period of time specified in the CP.

6.5 Certificate Distribution

The CA maintains controls to provide reasonable assurance that, upon issuance, complete and accurate certificates are available to subscribers and relying parties in accordance with the CA's disclosed business practices.

ILLUSTRATIVE CONTROLS

#	Certificate Distribution
6.5.1	The CA makes the certificates issued by the CA available to relevant parties using an established mechanism (e.g., a repository such as a directory) in accordance with the CP.
6.5.2	Only authorised CA personnel administer the CA's repository or alternative distribution mechanism.
6.5.3	The performance of the CA's repository or alternative distribution mechanism is monitored and managed.
6.5.4	The integrity of the repository or alternative distribution mechanism is maintained and administered.
6.5.5	Where required under privacy legislation, certificates are made available for retrieval only in those cases for which the subscriber's consent is obtained.

6.6 Certificate Revocation

The CA maintains controls to provide reasonable assurance that certificates are revoked, based on authorised and validated certificate revocation requests within the time frame in accordance with the CA's disclosed business practices.

ILLUSTRATIVE CONTROLS

#	Certificate Revocation
6.6.1	The CA provides a means of rapid communication to facilitate the secure and authenticated revocation of the following: a. one or more certificates of one or more subscribers; b. the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and c. all certificates issued by a CA, regardless of the public/private key pair used.
6.6.2	The CA verifies or requires that the RA verify the identity and authority of the entity requesting revocation of a certificate in accordance with the CP.
6.6.3	If an external RA accepts revocation requests, the CA requires that the RA submit signed certificate revocation requests to the CA in an authenticated manner in accordance with the CP.
6.6.4	If an external RA accepts and forwards revocation requests to the CA, the CA provides a signed acknowledgement of the revocation request and confirmation of actions to the requesting RA.
6.6.5	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms in the timeframes specified within the CP and in accordance with the format defined in ISO 9594/X.509 and ISO 15782-1.
6.6.6	The CA records all certificate revocation requests and their outcome in an audit log.
6.6.7	The CA or RA may provide an authenticated acknowledgement (signature or similar) of the revocation to the entity who perpetrated the revocation request.
6.6.8	Where certificate renewal is supported, when a certificate is revoked, all valid instances of the certificate are also revoked and are not reinstated.
6.6.9	The Subscriber of a revoked or suspended certificate is informed of the change of status of its certificate.

6.7 Certificate Suspension (if supported)

The CA maintains controls to provide reasonable assurance that certificates are suspended based on authorised and validated certificate suspension requests within the time frame in accordance with the CA's disclosed business practices.

Explanatory Guidance: Certificate Suspension is the process in which a certificate is effectively revoked for a 'temporary' period of time. Unlike revocation which is 'permanent' and can only be 'undone' by issuing a new certificate, suspension allows the certificate to be reinstated at a later period of time. During the time a certificate is suspended, it will appear on revocation lists, typically with a status of 'Certificate Hold'. CAs may only support Certificate Suspension for certain types of certificates.

ILLUSTRATIVE CONTROLS

#	Certificate Suspension
6.7.1	The CA provides a means of rapid communication to facilitate the secure and authenticated suspension of the following: a. one or more certificates of one or more subscribers; b. the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and c. all certificates issued by a CA, regardless of the public/private key pair used.
6.7.2	The CA verifies or requires that the external RA verify the identity and authority of the entity requesting suspension and reactivation of a certificate in accordance with the CP.
6.7.3	If an external RA accepts suspension requests, the RA submits signed certificate suspension requests to the CA in an authenticated manner in accordance with the CP.
6.7.4	The CA or RA notifies the Subscriber in the event of a certificate suspension.
6.7.5	Certificate suspension requests are processed and validated in accordance with the requirements of the CP.
6.7.6	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms upon certificate suspension. Changes in certificate status are completed in a time frame determined by the CP.
6.7.7	Certificates are suspended only for the allowable length of time in accordance with the CP.

#	Certificate Suspension
6.7.8	Once a certificate suspension (hold) has been issued, the suspension is handled in one of the following three ways: a. an entry for the suspended certificate remains on the CRL with no further action; b. the CRL entry for the suspended certificate is replaced by a revocation entry for the same certificate; or c. the suspended certificate is explicitly released and the entry removed from the CRL.
6.7.9	A certificate suspension (hold) entry remains on the CRL until the expiration of the underlying certificate or the expiration of the suspension, whichever is first.
6.7.10	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms upon the lifting of a certificate suspension in accordance with the CA's CP.
6.7.11	The CA verifies or requires that the external RA verify the identity and authority of the entity requesting that the suspension of a certificate be lifted.
6.7.12	Certificate suspensions and the lifting of certificate suspensions are recorded in an audit log.

6.8 Certificate Validation

The CA maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including Certificate Revocation Lists and other certificate status mechanisms) is made available to relevant entities (Subscribers and Relying Parties or their agents) in accordance with the CA's disclosed business practices.

Criterion	#	Certificate Validation
	6.8.1	The CA makes certificate status information available to relevant entities (Relying Parties or their agents) using an established mechanism in accordance with the CP. This is achieved using: a. Request Response Method – A request signed by the Relying Party to the Certificate Status Provider's responder. In turn, the Certificate Status Provider's responder responds with the certificate status duly signed. (OCSP is an example protocol using this method.) b. Delivery Method – A CRL signed by the CA and published within the policy's time frame.

Criterion	#	Certificate Validation
Certificate Revocation List (CRL) Controls	**6.8.2**	The CA digitally signs each CRL that it issues so that entities can validate the integrity of the CRL and the date and time of issuance.
	6.8.3	The CA issues CRLs at regular intervals, as specified in the CP, even if no changes have occurred since the last issuance.
	6.8.4	At a minimum, a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period.
	6.8.5	If certificate suspension is supported, a certificate suspension (hold) entry, with its original action date and expiration date remain on the CRL until the normal expiration of the certificate or until the suspension is lifted.
	6.8.6	CRLs are archived in accordance with the requirements of the CP including the method of retrieval.
	6.8.7	CAs include a monotonically increasing sequence number for each CRL issued by that CA.
	6.8.8	The CRL contains entries for all revoked unexpired certificates issued by the CA.
	6.8.9	Old CRLs are retained for the appropriate period of time specified in the CA's CP.
	6.8.10	Whether certificates expire, are revoked or are suspended, copies of certificates are retained for the appropriate period of time as disclosed in the CP.

Criterion	#	Certificate Validation
Online Certificate Status Protocol (OCSP) (or other online status mechanism) Controls	**6.8.11**	If an online certificate status collection method (e.g., OCSP) is used, the CA requires that certificate status inquiries (e.g., OCSP requests) contain all required data in accordance with the CP.
	6.8.12	Upon the receipt of a certificate status request (e.g., an OCSP request) from a Relying Party or its agent, the CA returns a definitive response to the Relying Party or its agent if: a. the request message is well formed; b. the Certificate Status Provider responder is configured to provide the requested service; c. the request contains the information (i.e., certificate identity – Serial number, OID, etc.) needed by the Certificate Status Provider responder in accordance with the CP; and d. the Certificate Status Provider's responder is able to locate the certificate and interpret its status. Where these conditions are met, the CA or Certificate Status Provider produces a signed response message indicating the certificate's status in accordance with the CP. If any of the above conditions are not met then a status of unknown may be returned.
	6.8.13	All response messages are digitally signed and include all required data in accordance with the CP.

7.0: Subordinate CA and Cross Certificate Lifecycle Management Controls

The Certification Authority maintains effective controls to provide reasonable assurance that subordinate CA certificate and cross certificate requests are accurate, authenticated and approved.

7.1 Subordinate CA Certificate and Cross Certificate Lifecycle Management

The CA maintains controls to provide reasonable assurance that:

- subordinate CA and cross certificate requests are accurate, authenticated and approved;
- subordinate CA and cross certificate replacement (renewal and rekey) requests are accurate, authorised, complete;
- new, renewed and rekeyed Subordinate CA and cross certificates are generated and issued in accordance with the CA's disclosed business practices;

- upon issuance, complete and accurate Subordinate CA and cross certificates are available to relevant entities (Subscribers and Relying Parties) in accordance with the CA's disclosed business practices;
- subordinate CA and cross certificates are revoked based on authorised and validated certificate revocation requests; and
- timely, complete and accurate certificate status information (including CRLs and other certificate status mechanisms) is made available to any entity in accordance with the CA's disclosed business practices.

Explanatory Guidance: A Subordinate CA certificate is a CA certificate issued by the Parent CA (typically using a Root CA) to a non-affiliated subordinate CA, typically to be operated under the Parent CA's CP. Cross certificates issued from one PKI to another are addressed are also addressed by this criterion.

ILLUSTRATIVE CONTROLS

Criterion	#	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.
	7.1.2	The Parent CA authenticates the Sub-CA or cross certificate request in accordance with the Parent's CP.
	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.
	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.
	7.1.7	The Parent CA authenticates the Sub-CA certificate rekey request in accordance with the CP.

Criterion	#	Subordinate CA Certificate and Cross Certificate Lifecycle Management
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.
	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.
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.
	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.

Appendix A: Business Practices Disclosure Topics

The CA maintains controls to provide reasonable assurance that its Certificate Policy and Certification Practice Statement address the topics from RFC 3647 or RFC 2527 listed below.

RFC 3647

Section No.	RFC 3647 Section
1	Introduction
1.1	Overview
1.2	Document Name and Identification
1.3	PKI Participants
1.3.1	Certification Authorities
1.3.2	Registration Authorities
1.3.3	Subscribers
1.3.4	Relying Parties
1.3.5	Other Participants
1.4	Certificate Usage
1.4.1	Appropriate Certificate Uses
1.4.2	Prohibited Certificate Uses
1.5	Policy Administration
1.5.1	Organisation Administering the Document
1.5.2	Contact Person
1.5.3	Person Determining CPS Suitability for the Policy

Section No.	RFC 3647 Section
1.5.4	CPS Approval Procedures
1.6	Definitions and Acronyms
2	Publication and Repository Responsibilities
2.1	Repositories
2.2	Publication of Certification Information
2.3	Time or Frequency of Publication
2.4	Access Controls on Repositories
3	Identification and Authentication
3.1	Naming
3.1.1	Type of Names
3.1.2	Need for Names to be Meaningful
3.1.3	Anonymity or Pseudonymity of Subscribers
3.1.4	Rules for Interpreting Various Name Forms
3.1.5	Uniqueness of Names
3.1.6	Recognition, Authentication, and Role of Trademarks
3.2	Initial Identity Validation
3.2.1	Method to Prove Possession of Private Key
3.2.2	Authentication of Organisation Identity
3.2.3	Authentication of Individual Identity
3.2.4	Non-Verified Subscriber Information
3.2.5	Validation of Authority

Section No.	RFC 3647 Section
3.2.6	Criteria for Interoperation
3.3	Identification and Authentication for Rekey Requests
3.3.1	Identification and Authentication for Routine Rekey
3.3.2	Identification and Authentication for Rekey After Revocation
3.4	Identification and Authentication for Revocation Request
4	Certificate Life Cycle Operational Requirements
4.1	Certificate Application
4.1.1	Who Can Submit a Certificate Application
4.1.2	Enrolment Process and Responsibilities
4.2	Certificate Application Processing
4.2.1	Performing Identification and Authentication Functions
4.2.2	Approval or Rejection of Certificate Applications
4.2.3	Time to Process Certificate Applications
4.3	Certificate Issuance
4.3.1	CA Actions During Certificate Issuance
4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate
4.4	Certificate Acceptance
4.4.1	Conduct Constituting Certificate Acceptance
4.4.2	Publication of the Certificate by the CA
4.4.3	Notification of Certificate Issuance by the CA to Other Entities
4.5	Key Pair and Certificate Usage

Section No.	RFC 3647 Section
4.5.1	Subscriber Private Key and Certificate Usage
4.5.2	Relying Party Public Key and Certificate Usage
4.6	Certificate Renewal
4.6.1	Circumstances for Certificate Renewal
4.6.2	Who May Request Renewal
4.6.3	Processing Certificate Renewal Requests
4.6.4	Notification of New Certificate Issuance to Subscriber
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate
4.6.6	Publication of the Renewal Certificate by the CA
4.6.7	Notification of Certificate Issuance by the CA to Other Entities
4.7	Certificate Rekey
4.7.1	Circumstances for Certificate Rekey
4.7.2	Who May Request Certification of a New Public Key
4.7.3	Processing Certificate Rekeying Requests
4.7.4	Notification of New Certificate Issuance to Subscriber
4.7.5	Conduct Constituting Acceptance of a Rekeyed Certificate
4.7.6	Publication of the Rekeyed Certificate by the CA
4.7.7	Notification of Certificate Issuance by the CA to Other Entities
4.8	Certificate Modification
4.8.1	Circumstances for Certificate Modification
4.8.2	Who May Request Certificate Modification

Section No.	RFC 3647 Section
4.8.3	Processing Certificate Modification Requests
4.8.4	Notification of New Certificate Issuance to Subscriber
4.8.5	Conduct Constituting Acceptance of Modified Certificate
4.8.6	Publication of the Modified Certificate by the CA
4.8.7	Notification of Certificate Issuance by the CA to Other Entities
4.9	Certificate Revocation and Suspension
4.9.1	Circumstances for Revocation
4.9.2	Who Can Request Revocation
4.9.3	Procedure for Revocation Request
4.9.4	Revocation Request Grace Period
4.9.5	Time Within Which CA Must Process the Revocation Request
4.9.6	Revocation Checking Requirements for Relying Parties
4.9.7	CRL Issuance Frequency
4.9.8	Maximum Latency for CRLs
4.9.9	Online Revocation/Status Checking Availability
4.9.10	Online Revocation Checking Requirements
4.9.11	Other Forms of Revocation Advertisements Available
4.9.12	Special Requirements re Key Compromise
4.9.13	Circumstances for Suspension
4.9.14	Who Can Request Suspension
4.9.15	Procedure for Suspension Request

Section No.	RFC 3647 Section
4.9.16	Limits on Suspension Period
4.10	Certificate Status Services
4.10.1	Operational Characteristics
4.10.2	Service Availability
4.10.3	Operational Features
4.11	End of Subscription
4.12	Key Escrow and Recovery
4.12.1	Key Escrow and Recovery Policy and Practices
4.12.2	Session Key Encapsulation and Recovery Policy and Practices
5	Facility, Management, and Operational Controls
5.1	Physical Controls
5.1.1	Site Location and Construction
5.1.2	Physical Access
5.1.3	Power and Air Conditioning
5.1.4	Water Exposures
5.1.5	Fire Prevention and Protection
5.1.6	Media Storage
5.1.7	Waste Disposal
5.1.8	Off-Site Backup
5.2	Procedural Controls
5.2.1	Trusted Roles

Section No.	RFC 3647 Section
5.2.2	Number of Persons Required per Task
5.2.3	Identification and Authentication for Each Role
5.2.4	Roles Requiring Separation of Duties
5.3	Personnel Controls
5.3.1	Qualifications, Experience, and Clearance Requirements
5.3.2	Background Check Procedures
5.3.3	Training Requirements
5.3.4	Retraining Frequency and Requirements
5.3.5	Job Rotation Frequency and Sequence
5.3.6	Sanctions for Unauthorised Actions
5.3.7	Independent Contractor Requirements
5.3.8	Documentation Supplied to Personnel
5.4	Audit Logging Procedures
5.4.1	Types of Events Recorded
5.4.2	Frequency of Processing Log
5.4.3	Retention Period for Audit Log
5.4.4	Protection of Audit Log
5.4.5	Audit Log Backup Procedures
5.4.6	Audit Collection System (Internal vs. External)
5.4.7	Notification to Event-Causing Subject
5.4.8	Vulnerability Assessments

Section No.	RFC 3647 Section
5.5	Records Archival
5.5.1	Types of Records Archived
5.5.2	Retention Period for Archive
5.5.3	Protection of Archive
5.5.4	Archive Backup Procedures
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
5.6	Key Changeover
5.7	Compromise and Disaster Recovery
5.7.1	Incident and Compromise Handling Procedures
5.7.2	Computing Resources, Software, and/or Data Are Corrupted
5.7.3	Entity Private Key Compromise Procedures
5.7.4	Business Continuity Capabilities After a Disaster
5.8	CA or RA Termination
6	Technical Security Controls
6.1	Key Pair Generation and Installation
6.1.1	Key Pair Generation
6.1.2	Private Key Delivery to Subscriber
6.1.3	Public Key Delivery to Certificate Issuer
6.1.4	CA Public Key Delivery to Relying Parties

Section No.	RFC 3647 Section
6.1.5	Key Sizes
6.1.6	Public Key Parameters Generation and Quality Checking
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)
6.2	Private Key Protection and Cryptographic Module Engineering Controls
6.2.1	Cryptographic Module Standards and Controls
6.2.2	Private Key (n out of m) Multi-Person Control
6.2.3	Private Key Escrow
6.2.4	Private Key Backup
6.2.5	Private Key Archival
6.2.6	Private Key Transfer Into or From a Cryptographic Module
6.2.7	Private Key Storage on Cryptographic Module
6.2.8	Method of Activating Private Key
6.2.9	Method of Deactivating Private Key
6.2.10	Method of Destroying Private Key
6.2.11	Cryptographic Module Rating
6.3	Other Aspects of Key Pair Management
6.3.1	Public Key Archival
6.3.2	Certificate Operational Periods and Key Pair Usage Periods
6.4	Activation Data
6.4.1	Activation Data Generation and Installation
6.4.2	Activation Data Protection
6.4.3	Other Aspects of Activation Data

Section No.	RFC 3647 Section
6.5	Computer Security Controls
6.5.1	Specific Computer Security Technical Requirements
6.5.2	Computer Security Rating
6.6	Life Cycle Technical Controls
6.6.1	System Development Controls
6.6.2	Security Management Controls
6.6.3	Life Cycle Security Controls
6.7	Network Security Controls
6.8	Time-Stamping
7	Certificate, CRL, and OCSP Profiles
7.1	Certificate Profile
7.1.1	Version Number(s)
7.1.2	Certificate Extensions
7.1.3	Algorithm Object Identifiers
7.1.4	Name Forms
7.1.5	Name Constraints
7.1.6	Certificate Policy Object Identifier
7.1.7	Usage of Policy Constraints Extension
7.1.8	Policy Qualifiers Syntax and Semantics
7.1.9	Processing Semantics for the Critical Certificate Policies Extension
7.2	CRL Profile
7.2.1	Version Number(s)

Section No.	RFC 3647 Section
7.2.2	CRL and CRL Entry Extensions
7.3	OCSP Profile
7.3.1	Version Number(s)
7.3.2	OCSP Extensions
8	Compliance Audit and Other Assessments
8.1	Frequency and Circumstances of Assessment
8.2	Identity/Qualifications of Assessor
8.3	Assessor's Relationship to Assessed Entity
8.4	Topics Covered by Assessment
8.5	Actions Taken as a Result of Deficiency
8.6	Communications of Results
9	Other Business and Legal Matters
9.1	Fees
9.1.1	Certificate Issuance or Renewal Fees
9.1.2	Certificate Access Fees
9.1.3	Revocation or Status Information Access Fees
9.1.4	Fees for Other Services
9.1.5	Refund Policy
9.2	Financial Responsibility
9.2.1	Insurance Coverage
9.2.2	Other Assets
9.2.3	Insurance or Warranty Coverage for End-Entities

Section No.	RFC 3647 Section
9.3	Confidentiality of Business Information
9.3.1	Scope of Confidential Information
9.3.2	Information Not Within the Scope of Confidential Information
9.3.3	Responsibility to Protect Confidential Information
9.4	Privacy of Personal Information
9.4.1	Privacy Plan
9.4.2	Information Treated as Private
9.4.3	Information Not Deemed Private
9.4.4	Responsibility to Protect Private Information
9.4.5	Notice and Consent to Use Private Information
9.4.6	Disclosure Pursuant to Judicial or Administrative Process
9.4.7	Other Information Disclosure Circumstances
9.5	Intellectual Property Rights
9.6	Representations and Warranties
9.6.1	CA Representations and Warranties
9.6.2	RA Representations and Warranties
9.6.3	Subscriber Representations and Warranties
9.6.4	Relying Party Representations and Warranties
9.6.5	Representations and Warranties of Other Participants
9.7	Disclaimers of Warranties
9.8	Limitations of Liability

Section No.	RFC 3647 Section
9.9	Indemnities
9.10	Term and Termination
9.10.1	Term
9.10.2	Termination
9.10.3	Effect of Termination and Survival
9.11	Individual Notices and Communications with Participants
9.12	Amendments
9.12.1	Procedure for Amendment
9.12.2	Notification Mechanism and Period
9.12.3	Circumstances Under Which OID Must be Changed
9.13	Dispute Resolution Provisions
9.14	Governing Law
9.15	Compliance with Applicable Law
9.16	Miscellaneous Provisions
9.16.1	Entire Agreement
9.16.2	Assignment
9.16.3	Severability
9.16.4	Enforcement (Attorney's Fees and Waiver of Rights)
9.17	Other Provisions

RFC 2527

Section No.	RFC 2527 Section
1	Introduction
1.1	Overview
1.2	Identification
1.3	Community and Applicability
1.3.1	Certification Authorities
1.3.2	Registration Authorities
1.3.3	End Entities
1.3.4	Applicability
1.4	Contact Details
1.4.1	Specification Administration Organisation
1.4.2	Contact Person
1.4.3	Person Determining CPS Suitability for the Policy
2	General Provisions
2.1	Obligations
2.1.1	CA Obligations
2.1.2	RA Obligations
2.1.3	Subscriber Obligations
2.1.4	Relying Party Obligations
2.1.5	Repository Obligations
2.2	Liability

Section No.	RFC 2527 Section
2.2.1	CA Liability
2.2.2	RA Liability
2.3	Financial Responsibility
2.3.1	Indemnification by Relying Parties
2.3.2	Fiduciary Relationships
2.4	Interpretation and Enforcement
2.4.1	Governing Law
2.4.2	Severability, Survival, Merger, Notice
2.4.3	Dispute Resolution Procedures
2.5	Fees
2.5.1	Certificate Issuance or Renewal Fees
2.5.2	Certificate Access Fees
2.5.3	Revocation or Status Information Access Fees
2.5.4	Fees for Other Services Such as Policy Information
2.5.5	Refund Policy
2.6	Publication and Repository
2.6.1	Publication of CA Information
2.6.2	Frequency of Publication
2.6.3	Access Controls
2.6.4	Repositories
2.7	Compliance Audit
2.7.1	Frequency of Entity Compliance Audit

Section No.	RFC 2527 Section
2.7.2	Identity/Qualifications of Auditor
2.7.3	Auditor's Relationship to Audited Party
2.7.4	Topics Covered by Audit
2.7.5	Actions Taken as a Result of Deficiency
2.7.6	Communications of Results
2.8	Confidentiality
2.8.1	Types of Information to be Kept Confidential
2.8.2	Types of Information Not Considered Confidential
2.8.3	Disclosure of Certificate Revocation/Suspension Information
2.8.4	Release to Law Enforcement Officials
2.8.5	Release as Part of Civil Discovery
2.8.6	Disclosure Upon Owner's Request
2.8.7	Other Information Release Circumstances
2.9	Intellectual Property Rights
3	Identification and Authentication
3.1	Initial Registration
3.1.1	Type of Names
3.1.2	Need for Names to be Meaningful
3.1.3	Rules for Interpreting Various Name Forms
3.1.4	Uniqueness of Names
3.1.5	Name Claim Dispute Resolution Procedure
3.1.6	Recognition, Authentication, and Role of Trademarks

Section No.	RFC 2527 Section
3.1.7	Method to Prove Possession of Private Key
3.1.8	Authentication of Organisation Identity
3.1.9	Authentication of Individual Identity
3.2	Routine Rekey
3.3	Rekey After Revocation
3.4	Revocation Request
4	Operational Requirements
4.1	Certificate Application
4.2	Certificate Issuance
4.3	Certificate Acceptance
4.4	Certificate Suspension and Revocation
4.4.1	Circumstances for Revocation
4.4.2	Who Can Request Revocation
4.4.3	Procedure for Revocation Request
4.4.4	Revocation Request Grace Period
4.4.5	Circumstances for Suspension
4.4.6	Who Can Request Suspension
4.4.7	Procedure for Suspension Request
4.4.8	Limits on Suspension Period
4.4.9	CRL Issuance Frequency (If Applicable)
4.4.10	CRL Checking Requirements
4.4.11	Online Revocation/Status Checking Availability

Section No.	RFC 2527 Section
4.4.12	Online Revocation Checking Requirements
4.4.13	Other Forms of Revocation Advertisements
4.4.14	Checking Requirements for Other Forms of Revocation Advertisements
4.4.15	Special Requirements re Key Compromise
4.5	Security Audit Procedures
4.5.1	Types of Events Recorded
4.5.2	Frequency of Processing Log
4.5.3	Retention Period for Audit Log
4.5.4	Protection of Audit Log
4.5.5	Audit Log Backup Procedures
4.5.6	Audit Collection System (Internal vs. External)
4.5.7	Notification to Event-Causing Subject
4.5.8	Vulnerability Assessments
4.6	Records Archival
4.6.1	Types of Records Archived
4.6.2	Retention Period for Archive
4.6.3	Protection of Archive
4.6.4	Archive Backup Procedures
4.6.5	Requirements for Time-Stamping of Records
4.6.6	Archive Collection System (Internal or External)
4.6.6	Procedures to Obtain and Verify Archive Information
4.7	Key Changeover

Section No.	RFC 2527 Section
4.8	Compromise and Disaster Recovery
4.8.1	Computing Resources, Software, and/or Data are Corrupted
4.8.2	Entity Public Key is Revoked
4.8.3	Entity Key is Compromised
4.8.4	Secure Facility After a Natural or Other Type of Disaster
4.9	CA Termination
5	Physical, Procedural, and Personnel Security Controls
5.1	Physical Controls
5.1.1	Site Location and Construction
5.1.2	Physical Access
5.1.3	Power and Air Conditioning
5.1.4	Water Exposures
5.1.5	Fire Prevention and Protection
5.1.6	Media Storage
5.1.7	Waste Disposal
5.1.8	Off-Site Backup
5.2	Procedural Controls
5.2.1	Trusted Roles
5.2.2	Number of Persons Required per Task
5.2.3	Identification and Authentication for Each Role
5.3	Personnel Controls
5.3.1	Background, Qualifications, Experience, and Clearance Requirements

Section No.	RFC 2527 Section
5.3.2	Background Check Procedures
5.3.3	Training Requirements
5.3.4	Retraining Frequency and Requirements
5.3.5	Job Rotation Frequency and Sequence
5.3.6	Sanctions for Unauthorised Actions
5.3.7	Contracting Personnel Requirements
5.3.8	Documentation Supplied to Personnel
6	Technical Security Controls
6.1	Key Pair Generation and Installation
6.1.1	Key Pair Generation
6.1.2	Private Key Delivery to Entity
6.1.3	Public Key Delivery to Certificate Issuer
6.1.4	CA Public Key Delivery to Users
6.1.5	Key Sizes
6.1.6	Public Key Parameters Generation
6.1.7	Parameter Quality Checking
6.1.8	Hardware/Software Key Generation
6.1.9	Key Usage Purposes (as per X.509 v3 Key Usage Field)
6.2	Private Key Protection
6.2.1	Standards for Cryptographic Module
6.2.2	Private Key (n out of m) Multi-Person Control
6.2.3	Private Key Escrow

Section No.	RFC 2527 Section
6.2.4	Private Key Backup
6.2.5	Private Key Archival
6.2.6	Private Key Entry Into Cryptographic Module
6.2.7	Method of Activating Private Key
6.2.8	Method of Deactivating Private Key
6.2.9	Method of Destroying Private Key
6.3	Other Aspects of Key Pair Management
6.3.1	Public Key Archival
6.3.2	Usage Periods for the Public and Private Keys
6.4	Activation Data
6.4.1	Activation Data Generation and Installation
6.4.2	Activation Data Protection
6.4.3	Other Aspects of Activation Data
6.5	Computer Security Controls
6.5.1	Specific Computer Security Technical Requirements
6.5.2	Computer Security Rating
6.6	Life Cycle Technical Controls
6.6.1	System Development Controls
6.6.2	Security Management Controls
6.6.3	Life Cycle Security Controls
6.7	Network Security Controls
6.8	Cryptographic Module Engineering Controls

Section No.	RFC 2527 Section
7	Certificate and CRL Profiles
7.1	Certificate Profile
7.1.1	Version Number(s)
7.1.2	Certificate Extensions
7.1.3	Algorithm Object Identifiers
7.1.4	Name Forms
7.1.5	Name Constraints
7.1.6	Certificate Policy Object Identifier
7.1.7	Usage of Policy Constraints Extension
7.1.9	Processing Semantics for the Critical Certificate Policies Extension
7.2	CRL Profile
7.2.1	Version Number(s)
7.2.2	CRL and CRL Entry Extensions
8	Specification Administration
8.1	Specification Change Procedures
8.2	Publication and Notification Policies
8.3	CPS Approval Procedures